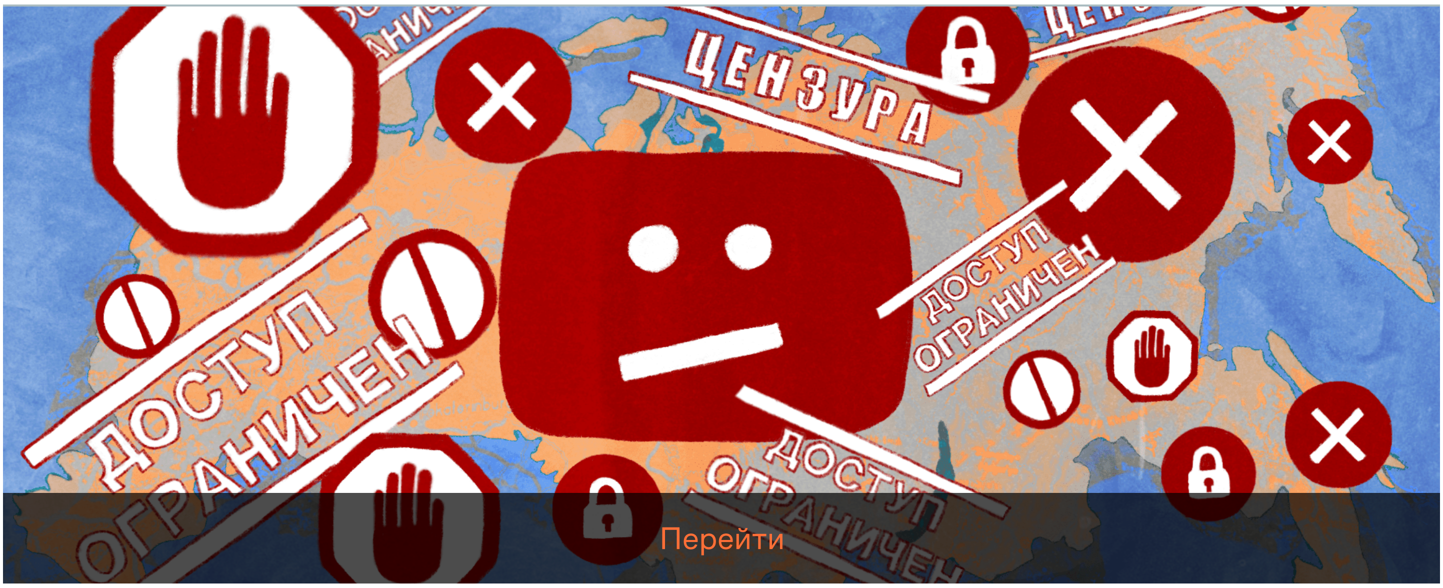


Иллюстрация: Саша Филатова для ОВД-Инфо

07.06.2022

Internet blocks as a tool of political censorship

Date of publication: June, 7, 2022
Текст на русском: Блокировки интернет-ресурсов как инструмент политической цензуры

Over the past ten years, blocking has become one of the largest tools for restricting access to information and freedom of expression. Although the first legislative changes expanding the possibilities of blocking and simplifying this procedure appeared back in 2012, there have still been very few studies and reports on the situation, and it has not received wide public coverage outside narrow human rights and expert circles for a long time. The lack of proper documentation of violations of international norms and human rights standards only contributes to the current situation — de facto complete Internet censorship in relation to alternative sources of information.

As has been repeatedly emphasized by various experts and institutions, the Internet is one of the key technologies for the rapid and decentralized exchange of information, where responsibility for the content of publications is also distributed among different units. This makes the Internet fundamentally different from traditional media. This, as well as the availability of technology to ordinary users, have made the web the main means of expressing opinions at the present time. Nevertheless, the authorities of different countries, including Russia, are trying to appropriate control over the Internet within state borders — they restrict the use of foreign servers, force large IT companies to open offices in the country, place equipment at cross-border exchange points that blocks certain sources of information, etc.

In this report, we consider blocking Internet resources as a tool of political censorship, connected, on the one hand, with the general policy of bans on freedom of speech in Russia, and on the other, with network technologies that are fundamentally different from traditional media.
We consider online censorship in its dynamics: we compare the current situation of the war and the radical measures implemented to restrict freedom of speech in Russia, with the beginning of 2022, when all the main tools of online censorship have already developed, and also trace the history of the formation of legislative instruments and law enforcement practice of the last ten years.

The report is based on the following sources:

- Legislation of the Russian Federation affecting freedom of speech on the Internet (laws «On Information», «On the protection of children from harmful Information», «On the media», «On measures to influence persons involved in violations of fundamental human rights and freedoms» and others);

- Roskomnadzor documents (activity reports, press releases, etc.);

- The European Convention on Human Rights, the International Covenant on Civil and Political Rights, and other international documents;

- Practice of the European Court of Human Rights, opinions of the Venice Commission;

- Documents of the UN Human Rights Committee, the UN Human Rights Council, UN Special Rapporteurs, the Organization for Security and Co-operation in Europe, the European Union, the Organization of American States, the African Commission on Human and Peoples' Rights, Inter-American Commission on Human Rights, and other international organizations;

- The OVD-Info report «No to war. How Russian authorities are suppressing anti-war protests, » and other materials and data from OVD-Info;

- Reports of Russian and international NGOs on freedom of speech and blocks, other documents and statements (the project «Misuse of Anti-extremism» of the SOVA Center, the Net Freedoms Project of the Agora International Human Rights Group, as well as Human Rights Watch, Amnesty International, Civil Rights Defenders, Reporters Without Borders, Accessnow, CIVICUS, Article 19, Freedom House, Censored Planet, and others);

- Data of the Roskomsvoboda project (register of blocked resources, news, expert comments);
- Publications of the Mass Media Defence Center;
- Publications in the media (RBC, Cnews.ru, news section of the OVD-Info website);
- A closed round table organized by OVD-Info with the participation of experts from the projects SOVA, Roskomsvoboda, Net Freedoms Project, and Mass Media Defence Center.

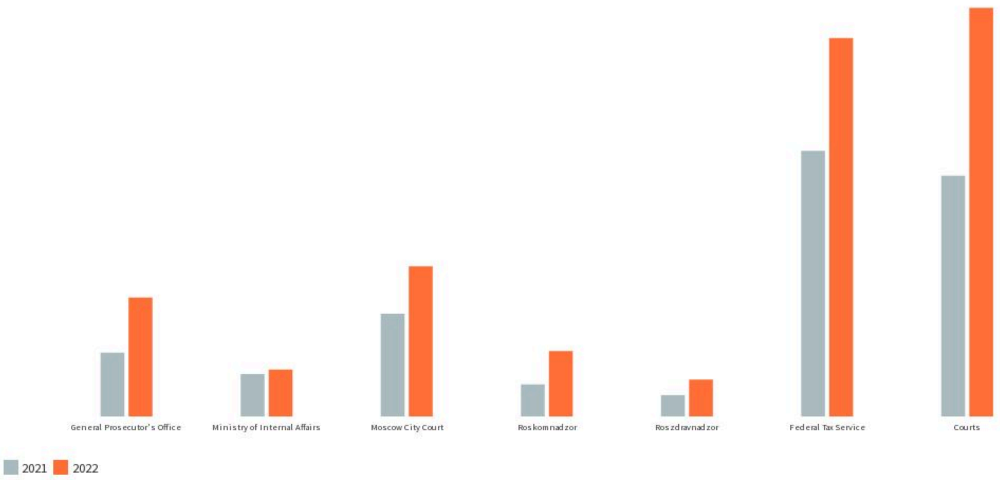
Blocking Internet resources in Russia

One of the main and obvious problems of resource blocking in Russia is its constantly growing scale. It was not always associated with political censorship, but it seriously affected the general possibility of expressing opinions and the development of civil society. The trend is perfectly traced by the increase in the number of blocked resources, as well as the reasons for such blocks. In fact, according to the Roskomsvoboda project, **261** resources were blocked in 2012, whereas in 2021, **63 554** resources were blocked at the request of the courts, and another **8421** — at the request of Roskomnadzor.

According to the Network Freedoms project, in 2021, there were more than **450 thousand** specific cases of interference with Internet freedom in Russia (most of them — blocks) and more than **90** general initiatives on restrictions and bans on the Internet. These figures are enough to understand that blocks are a large-scale measure, the indicators of which have been constantly growing since 2012 and until February 24, 2022, when an avalanche of blocks actually destroyed direct access from Russia to non-state socio-political media. Moreover, the trends of recent years include not only an increase in the number of blocks, but also the criminalization of online activity, as the Net Freedoms Project writes in the report on Internet freedoms for 2020. Users are increasingly receiving fines and prison sentences for their texts, reposting other people's materials and even likes.

The situation only worsened with the outbreak of the war. From February 24 to May 5, according to Roskomsvoboda, more than **3,000 sites** were censored in connection with publications about the war (it is important that this statistic does not include blocking on other grounds). New bills restricting freedom of speech for both the media and citizens were introduced and came into force; many media outlets were blocked or dissolved; social networks were «slowed down» or declared «extremist» and banned. According to Roskomnadzor, about **120 thousand** resources were also blocked, among which the RKN allegedly found not only «fakes, » but also sites with «Ukrainian nationalist propaganda with a total audience of over 202 million users.»

The number of blocks from February 24 to May 26, 2022, rose
in comparison with the same period of 2021



Source: Roskomsvoboda • By May 30, 2022

Made with Flourish • Create your own

According to the list of blocked resources of Roskomsvoboda, the number of blocks from February 24 to May 26, 2022 increased for almost all agencies compared to the same period in 2021. In particular, a large increase is due to blocking by the decision of the Prosecutor General's

Office, that is, as a rule, related to the restriction of political freedoms.

The state information policy is still formally based on legislation, but the range of laws adopted in recent years allows authorities to block almost any page, website or media. The latest amendments proposed to the State Duma, if they are adopted, will allow Roskomnadzor to do this without a court decision, only at the request of the Prosecutor General's Office — that is, lightning fast.

Blocking may not be the most painful way of infringing on freedoms, but it is definitely the most widespread. According to our roundtable experts, as well as to the results of the study of the most notable cases of blocking over the past two years, one can consider purely political the bans on «calls to participate in mass (public) events held in violation of the established procedure, » on the publication of materials of «undesirable organizations, » and after the outbreak of the war, on publication of «unreliable socially significant information» (for more information, see the chapter «Blocking and civil liberties»). Most of the other justifications listed in the law «On information» can be used both to ban child pornography or drug sales, and for political repression. According to experts, blocking by the decision of the Prosecutor General's Office (in particular, under Article 15.3 of the Law «On information») is more often a restriction of political freedoms than blocking on other grounds — such as illegal sale of alcohol or documents, information about drugs, publications about suicide, or pornography involving minors. This is how the lawyer and legal analyst of the Agora group, Damir Gainutdinov, describes these mechanisms: *«Generally, in all prosecutor's blockings the resource shutdown comes first, and only then the website owner is notifiedand gets the opportunity to exit the Unified Domain Name Registry and plead for unblocking. That is, prosecutors are engaged in the most socially dangerous and important decisions on blocks. Where we are talking about drugs,* *suicide, pornography and alike, authorities first notify the owner of the resource, then wait a day until the owner deletes the banned information, and only then put the site in the Registry if it is not deleted. And if the resource is blocked by prosecutors, they immediately put it into the Register and block it, and only after that the owner of the resource is notified. The prosecutors' topics are calls for protests, fake news, and so on.»*

The blocking of publications by political opposition institutions (and not individual pages or websites) is usually the result of centralized political decisions. In this case, the bans are not related to the content of specific publications, but to their belonging to an institution that has become a target of political repression — Anti-Corruption Foundation (FBK), Open Russia, Team 29, Project, etc. Such blocks are always accompanied by other restrictions, up to criminal cases. Galina Arapova (Mass Media Defense Center) gives an example of the understanding of the term «mirror», which is used by Russian courts and the Prosecutor General's Office: «*Law enforcement agencies and courts understand „mirrors" a little awry*, » says Arapova.«*It doesn't matter what content is there, but if a site has a connection with an organization that they want to block, then it is considered a mirror. Even if it is called differently and the content on it is different. This makes it possible to apply quite arbitrarily to new sites the decision that was made earlier on another occasion and for other content*.»

Since 2012, the Russian authorities have been creating and developing a legislative framework for the possibility of unlimited blocking — only to the law «On Information, » **84** amendments have been made over the past two years. Simultaneously, the regulators (Roskomnadzor and others) ordered the development of technologies for automated control over the dissemination of information on the Internet. Finally, the mechanisms of blocking (judicial and extrajudicial) were worked out — for individual pages, entire sites and domains; with the possibility of unblocking, «slowing down» and full domain revocation, etc.

If until February 24, 2022, the blocks could take place in different ways — with and without notification, with the ability to delete content and retain access to the resource — then immediately after the outbreak of the war, most of the blocks began to occur immediately and extrajudicially, on the basis of Article 15.3 of the law «On Information».

INTERNET AND CENSORSHIP

In February 2016, the then head of Roskomnadzor, Alexander Zharov, commented on the frequent accusations of censorship against the agency: «*Censorship involves reviewing an article or other information even before it is broadcast or printed. And we react after the fact. Therefore, we do not have any censorship*.» According to the Constitution of the Russian Federation, which Zharov also quoted, censorship is prohibited in Russia. The question, however, is how exactly it is defined. The Law «On Mass Media» of 1991 (Article 3) provides the following definition: «*... the requirement from the editorial office of a mass media outlet on the part of officials, state bodies, organizations, institutions, or public associations, to pre-coordinate messages and materials (except in cases when the official is the author or the interviewee), as well as the imposition of a ban on the distribution of messages and materials, their individual parts...*».

The «requirement... to pre-coordinate messages» refers to the Soviet censorship system and, accordingly, to the traditional press — television, radio and newspapers. This algorithm is technically unrealizable in the case of publications on the Internet: access to it is democratic, and total control of the content of messages before their publication is impossible. However, the second part of the definition from the same article, namely «the imposition of a ban on the distribution of messages and materials, » can be understood as a separate type of censorship, which directly refers to the blocking of Internet resources. In 2010, the Supreme Court issued the plenum resolution «On the practice of application by courts of the Law of the Russian Federation „On Information", » in which it defined written warnings, as well as the imposition by the court of a ban on the production and release of mass media as «not censorship.» According to the resolution, such bans are «established by federal laws in order to prevent abuse of freedom of the media.» Thus, it can be said that there is systematic censorship in Russia, which is carried out by the authorities and which is not recognized by them as such.

Without calling its own actions «censorship, » the state, nevertheless, uses this term to define the policy of global Internet platforms that restrict access to official Russian channels and accounts. Thus, the word «censorship» appears in the explanatory note to the bill «On Amendments to the Federal Law „On Measures of Influence on Persons Involved in Violations of Fundamental Human Rights and Freedoms, the Rights and Freedoms of Citizens of the Russian Federation"» (adopted in December 2020 under the number 481-FZ):

> **«In fact, since April 2020, the authorized agencies of the Russian Federation have been recording complaints from the editorial offices of the media outlets about the facts of censorship of their accounts by foreign Internet platforms Twitter, Facebook and Youtube. Such media outlets as Russia Today, RIA Novosti, Crimea 24, were censored. In total, about 20 facts of discrimination were recorded.»**

This is not really about state censorship, but about the policy of commercial corporations. However, it has a special definition in the law «on censorship»: «*... a restriction by the owner of an Internet resource on the dissemination by users of... socially significant information on the territory of the Russian Federation»* if it *«violates the right of citizens of the Russian Federation to freely seek, receive, transmit, produce and distribute information.»* In response to such «censorship» Roskomnadzor blocks foreign Internet sites and social networks.

If in Russia the concept of «censorship» is used only in relation to foreign platforms, then in European and, more broadly, Western judicial practice it occurs in the context of Russian information policy. In the case OOO Flavus and Others v. Russia, in which the ECHR in 2020 decided that the Russian law «On Information» and the practice of blocks violates two articles of the Convention for the Protection of Human Rights and Fundamental Freedoms at once, one of the invited experts in his commentary («third-party intervention») calls widespread blocking of sites «digital censorship.» However, this is rather an exception — in the decisions of the court itself on cases of blocks in Russia, the term «censorship» is not used.

This term is much more common in international human rights practice. For example, Special Rapporteurs on freedom of expression in their declarations label as «pre-censorship» the Internet content filtering systems that are not controlled by end users (p. 88). International human rights NGOs and activists in the field of freedom of speech understand this term even more broadly and actively use it in reports on Russian policy towards the Internet.

Before Russia invaded Ukraine, monitoring and reports focused on the routine practice of Roskomnadzor. Thus, the terms «censorship», «online censorship», «Internet censorship», etc. have appeared in Human Rights Watch's 2017, 2020 and 2021 reports, as well as in Freedom House and Censored Planet reports. In particular, the authors of Censored Planet noted that against the background of the growth of cyber censorship around the world, «including in reportedly „free“ countries, » the Russian example is particularly noteworthy: «*A country that once had very little censorship has been thrust into the spotlight due to… their steadily growing blocklist*.»

The policy of the Russian authorities towards the Internet contradicts its technological essence. As the authors of the report on the Russian regulation of the Internet by the Censored Planet project note, the distribution and decentralization of networks is no longer a guarantee of the protection of freedom of speech. «*It was long thought that large-scale censorship on decentralized networks like Russia, United States, India and the United Kingdom was prohibitively difficult*, » they write. «*Our exhaustive study of Russia's censorship infrastructure shows that that is not the case*.» In their opinion, «naive» censorship gave way to advanced technologies when Roskomnadzor became able to centrally manage traffic routing thanks to the law «on the sovereign Runet» (see the chapter «The Sovereign Runet»).

Experts of the Roskomsvoboda project disagree with the authors of the report. In fact, at a closed round table on Internet blocks held by OVD-Info on February 8, 2022, the head of Roskomsvoboda, Artem Kozlyuk, expressed a different position from Censored Planet. «*The Internet was specially created using such protocols to avoid unnecessary limits and blocks*, » Kozlyuk said. «*So that each bit reaches the end it is intended for. If there are any restrictions on the path of this bit, it will still try to reach the endpoint. Online censorship contradicts the principle of the Internet. Yes, there will be a struggle of technologies, but banned information will always be distributed — if not through one, then through other channels.*»

After February 24, when mass blocking of media outlets, individual posts and accounts of activists and human rights defenders began, and new articles of the Administrative Offense Codes and the Criminal Code were adopted, making it liable offenses to «discredit» and «distribute unreliable information» about the Russian armed forces, many experts and observers began to talk about «military censorship.» In fact, in the latest ranking of freedom of speech, the authors of Reporters Without Borders separately pay attention to the situation in Russia, which has dropped from 150th place to 155th: «*In Russia, the government has taken complete control of news and information by establishing extensive wartime censorship, blocking the media, and pursuing non-compliant journalists, forcing many of them into exile*.»

The Network Freedoms project has created a map of Russian cities where people were held liable under the new Article 20.3.3 of the Code of Administrative Offenses, calling it a «Map of military censorship.» The Roskomsvoboda project also describes the situation, publishing data on the blocks of websites for «fakes» about the Russian army (as of May 5, 2022, there were 3,000 such blocks).

LEGISLATION ON INTERNET BLOCKING

From amendments to the law «On the Protection of Children from Information» to the complete isolation of the Runet

Formal conditions for the start of the Internet resource blocking were created in 2012 by amendments to the law «On the Protection of Children from Information Harmful to their Health and Development» (139-FZ). Then definitions of Internet-related terms («website, » «page, » «domain name, » «network address, » «hosting provider, » «site owner») were introduced into the legislation, " and the Unified Register» and the agency responsible for it, Roskomnadzor, were created. In 2012, the thematic definition of materials, access to which should be blocked by a court decision (Article 15.1, dedicated to the Register), was limited to pornography involving minors, information about ways to commit suicide, as well as about the manufacture or purchase of drugs. However, even then a clause was formulated that did not relate to the protection of children: «information *prohibited for dissemination in the Russian Federation on the basis of a court decision that entered into force on the recognition of information as prohibited for dissemination*.» That is, information recognized by the court as extremist and included in the Federal List of Extremist Materials.

Although it was about the protection of children, which implied a public consensus, activists and experts expressed concern about the new law, which, in their opinion, could be used to restrict freedom of speech. In addition, together with this law, a number of other laws were passed restricting political freedoms — from a sharp increase in fines for participating in «unauthorized rallies» to the law on «foreign agents.»

Indeed, after a number of amendments, the law 149-FZ «On Information» began to be used to block a wide range of resources. The most radical changes were made at the end of 2013 by the Lugovoi Law (398-FZ). Then Article 15.3 appeared, which introduced extrajudicial blocking for «extremism, » namely, for «*information containing calls for mass riots, extremist activities, participation in mass (public) events held in violation of the established procedure…*» Thus, a ban on the dissemination of certain types of information that was introduced in order to protect children, gradually turned into a multi-tool for restricting freedoms.

The Lugovoi Law also described the blocking mechanism, which includes a long chain: at the request of the Prosecutor General or his deputies, Roskomnadzor requires the erasure of information from the telecom operator and notifies the hosting provider; the operator restricts access to the resource, and the hosting provider informs the owner of the resource about the requirement to delete information; after the information is deleted and Roskomnadzor is notified about it, the agency allows the telecom operator to unblock the resource. At the same time, there was no clear indication in the law what exactly is being blocked — a page, domain or IP. As a result, other resources that are thematically unrelated to the object of the ban and belong to other people were often blocked by domain and IP.

Employees of organizations and site owners either did not receive any notifications at all, or received letters from Roskomnadzor, which did not specify which information published on the site contradicts the law. Moreover, such a norm was originally laid down in the Lugovoi Law, according to which the Prosecutor General is not obliged to inform the owners about the reasons for which their sites were blocked.

According to the SOVA Center for Information and Analysis, among the first fifteen resources blocked under the Lugovoi Law in 2014, together with the Islamist sites (Hunafa.info, VDagestan.com, Daymohk), there were online publications Yezhednevnyy Zhurnal, Kasparov.ru and Grani.ru, several websites with news about the march for the federalization of Siberia, the article «The Appeal of Right Sector to the peoples of Russia, » as well as the blog of Alexei Navalny and its 28 mirrors.

By 2021, Lugovoi Law had become the main legislative instrument of censorship: for example, the wording «calls for mass riots, extremist activities» from Article 15.3 allowed the blocking by the decision of the Prosecutor General's Office of the sites of the «Team 29», several sites supported by Mikhail Khodorkovsky («Open Media», «MBH Media», «Pravozashita Otkrytki, » duma.vote), as well as dozens of sites related to the activities of Alexey Navalny (Lyubov

Sobol’s and Navalny LIVE channel, Georgy Alburov’s, Leonid Volkov’s and Vladimir Milov’s, even earlier, in 2018 — navalny.com).

In 2017, the law on «Mass Media-foreign agents» (327-FZ) amended the law «On Mass Media» — the concept of «foreign mass media performing the functions of a foreign agent» appeared in Article 6. The same law also made further amendments to the law «On Information»: the list of grounds for extrajudicial blockages (Article 15.3) was supplemented with the wording «*information materials of a foreign or international non-governmental organization whose activities are recognized as undesirable on the territory of the Russian Federation*» (the law on «undesirable organizations» (129-FZ) was adopted two years earlier, in 2015)*.* Under this pretext — the materials of an «undesirable organization» — in 2021, the pages with investigations of the «Project» and «Open Media» were blocked. In addition, the following wording also appeared in Article 15.3: «*information allowing access to the specified information or materials*.» What kind of information, the law did not specify, and experts interpreted it as ordinary hyperlinks. In the expert opinion of the Human Rights Council on the law on «Media-foreign agents», the director of the SOVA Center for Information and Analysis, Alexander Verkhovsky, noted that such wording could lead to mass blocking of any pages, websites, as well as blogs and social networks. Media outlets, bloggers and ordinary users of social networks for many years published links to the materials of organizations that were not considered «undesirable» at that time. «*Thus*, » Verkhovsky writes, «*the introduction of this rule means giving the Prosecutor General’s Office an almost unlimited opportunity to block access to a huge number, possibly to the majority, of websites and blogs, at least of socio-political subjects. But such powers of extrajudicial sanctions cannot in any way be considered proportional to the issues that, according to the explanatory note, the bill is intended to solve*.»

In the same year, 2017, but a few months earlier, other amendments to the law «On Information» (276-FZ) were adopted, introducing Article 15.8. It described «*measures aimed at countering the use of information and telecommunication networks and information resources on the territory of the Russian Federation, through which access is provided to information resources and information and telecommunication networks, access to which is restricted on the territory of the Russian Federation*.» Both the press and Roskomnadzor perceived this as a ban on the use of VPNs and anonymizers to bypass blocks. Shortly after the publication of the law, Roskomnadzor demanded from companies that provide the possibility of using VPNs and anonymizers to register in the FGIS system, which provides access to the register of prohibited Internet resources. This allows one to track whether anonymizers add addresses of blocked sites to the blacklist.

Almost 10 years of legislative activity were spent on amendments to the law «On Information», which continued to expand the list of prohibited types of information, describe and codify those responsible for its publication and blocking, and also toughened penalties for violating the law:

- In 2018, Law 472-FZ introduced another «children's» clause into Article 15.1 (on the register) — on «*inciting minors to commit illegal actions*.» In 2021, this wording allowed the Investigative Committee to open a criminal case against Leonid Volkov for calling for participation in «unauthorized» rallies in support of Alexei Navalny.

- On March 18, 2019, the law 30-FZ was adopted, amending the law «On Information». The new article 15.1.1 is called «*The procedure for restricting access to information expressing in an indecent form, that offends human dignity and public morality, obvious disrespect for society, the state, official state symbols of the Russian Federation, the Constitution of the Russian Federation, or bodies exercising state power in the Russian Federation.*» In fact, this has become an extension of the scope of the «Lugovoi Law», since the mechanism for blocking websites, pages and blogs under this article does not differ from the mechanism for blocking «extremist» materials: access restriction occurs at the request of the Prosecutor General or their deputies, and Roskomnadzor is responsible for it. The Mass Media Defence Center notes that this wording is extremely vague and does not give an understanding of what exactly can be considered an «indecent form, » as well as what exactly is meant by «bodies exercising state power.» For example, in the 2019 case of insulting the governor of the Arkhangelsk Region, the Supreme Court clarified that «the president, the Federal Assembly (the State Duma and the Federation Council), the government and the courts are considered to be [such] bodies. In the regions, local authorities — assemblies of deputies and governments — are added to them.» That is, governors do not belong to this list — however, courts in their practice often include the police and the FSB in the concept of «bodies exercising state power.»

- On the same day, Law 31-FZ was adopted, which introduced the concept of «unreliable socially significant information, » the dissemination of which is also punished by extrajudicial blocking (under Article 15.3). Moreover, this wording applies only to online publications, which do not include, for example, «news aggregators» and traditional media, but include the sites of these media, as well as sites registered as online publications. In this case, the materials are blocked according to a special algorithm: the Prosecutor General informs Roskomnadzor, the latter informs the editorial office of the online publication, and the telecom operator appears in the chain only if the editorial office has not deleted the material and it needs to be blocked. Both the press and the legislators themselves called this law the «Fake News Law.» At the same time, amendments were made to the Administrative Offense Codes (part 9 of Article 13.15), which introduced fines for publishing «unreliable socially significant information» (the penalties were tightened next year). After February 24, this law, with subsequent amendments to the Administrative Offense Codes and the Criminal Code, became the main instrument of military censorship.

According to Damir Gainutdinov, the law on «fakes» was in practice not used until 2020 — then it began to be massively applied against resources publishing «false information» about the coronavirus: *«During this time, practice has developed, explanations of the Supreme Court have appeared on how to apply it, and now on this basis it is applied to information about the war.»* A signature case is the blocking of the resource «Taiga.info» two weeks before the start of the war: the site published an article about food shortages in the village of Khatanga on Taimyr, after which this text was blocked on the grounds of violating the article on «fakes.» The Agora group managed to appeal this blocking, but two weeks later the website «Taiga.info» was blocked completely — with the same justification, but this time for covering the war.

- In the same 2019, Law 426-FZ introduced the requirement of mandatory labeling of «foreign agents, » the absence of which may also be punished by blocking of the resource (Article 15.8).

- In 2020, four new laws were adopted, which introduced 64 amendments to the law «On Information, » but most of these edits were devoted to financial security (FZ 479), information on the illegal sale of medicines (FZ 105), and other topics not directly related to political rights.
  In December of the same year, the «law on censorship» (482-FZ) was adopted, which allowed Roskomnadzor to block or slow down Internet platforms if they restrict the dissemination of «socially significant information.»

The last changes in the substantive part of the law (that is, in the enumeration of the types of information, the publication of which may lead to a block) were made already in 2021:

- Law 43-FZ introduced a new article 15.3-1, according to which websites with election campaigning and other election information may be subject to extrajudicial blocking if the content contradicts the law. In this case, the election commission has the right to initiate blocking by making a request to Roskomnadzor, which, in its turn, makes a request to a telecom operator. That is, the site is blocked at first, and only afterwards its owner can delete the information and request unblocking.

- Law 260-FZ for 2021 introduced a new article 15.1-2: «*The procedure for restricting access to false information that discredits the honor and dignity of a citizen (individual) or* undermines *their reputation and is associated with the accusation of a citizen (individual) of committing a crime.»* The article describes the mechanism: a citizen who finds false information about themselves writes a plea addressed to the prosecutor, after which the prosecutor's office checks the information for authenticity and, in case of violation, sends a notification to Roskomnadzor, which notifies the hosting provider, and the provider, in turn, notifies the site owner. If the information is not deleted by the owner within a day, the site is blocked by the telecom operator.

- Law 288-FZ, adopted on the same day as the previous one (260-FZ), added to Article 15.1 (on the register) another type of information for which a website or page is blocked: confidential information about judges, officials, and law enforcement agencies.

- Law 250-FZ added to Article 15.3 (on extrajudicial blocking) a clause on the resources of financial fraudsters — such as imitation of official bank websites, as well as sites that «encourage participation in financial pyramids.» In this case, the blocking may occur at the initiative of the Bank of Russia.

- In December 2021, Law 441-FZ was adopted, which expanded the grounds for extrajudicial blocks (Article 15.3) by introducing four new points: from that moment on, not only «calls for mass riots and the carrying of extremist activities» were banned, but also «justification and (or) rationale for the carrying of extremist activities, including terrorist activities»; «false reports of acts of terrorism»; materials of organizations recognized as terrorist or extremist and links to them; as well as «an offer to purchase a forged document granting rights or releasing from obligations.»

After Russia's invasion of Ukraine, the state information policy sharply tightened. However, most of the legislative tools for quickly blocking unwanted publications had already been created by this time, so between February 24 and May 28, mainly those bills were submitted to the State Duma and adopted that clarified the wordings and introduced new penalties for publications — fines and prison terms.

So, on March 4, 2022, laws 31 FZ and 32 FZ were adopted, which added to the Administrative Offense Code and the Criminal Code articles on «discrediting the use of the Armed Forces of the Russian Federation, » «calls for the introduction of restrictive measures against the Russian Federation» (that is, sanctions), *as* well as on «public dissemination of deliberately false information about the use of the Armed Forces of the Russian Federation» (Articles 20.3.3 and 20.3.4 of the Code of Administrative offenses; Articles 280.3 and 284.2 of the Criminal Code). On March 22, 2022, amendments were made to these articles, which added to the list of illegal actions «discreditation» and «dissemination of false information about the work of Russian state bodies abroad.» If the «public dissemination of deliberately false information» about the use of the Russian army or about the actions of state bodies abroad entailed «grave consequences, » then the punishment can be up to 15 years in prison — this is the toughest of the laws adopted after February 24, 2022.

In practice, this led to the fact that individual authors and entire editorial offices deleted their publications themselves or announced a complete refusal to cover military operations.

On April 6, a bill on the extrajudicial termination of the work of media outlets by the decision of the Prosecutor General's Office was introduced in the State Duma, giving the Prosecutor General's Office the right to close Russian media outlets without judicial intervention and initiate a ban on foreign media working in Russia. The initiators of the bill called these measures «mirroring, » referring to the blocking of official Russian media on foreign platforms (Youtube, Facebook, etc.) that have become more frequent after the outbreak of the war. At the time of writing, this bill has been approved in the first reading.

According to the bill, the Prosecutor General's Office will be able to declare the registration of any media invalid if it is found to:

- spread «fakes» or information that «offends human dignity and public morality»;
- «express obvious disrespect for society, the state, official state symbols of the Russian Federation, the Constitution, state authorities»;
- disseminate information containing «calls to participate in unauthorized public events» or to impose sanctions;
- contain propaganda, justification or defence of «extremist activity».

In this case, the activities of the media outlet will be banned, and employees will lose their accreditation.

Moreover, this bill provides for the extrajudicial blocking of websites containing «false information disseminated under the guise of reliable reports» about the use of the armed forces, the activities of government agencies abroad, as well as their discreditation or calls for sanctions. After the adoption of the new amendments, the Prosecutor General's Office, with the «repeated dissemination of such information, » will have the right to send a request to Roskomnadzor for the immediate blocking of the site, as well as resources «confusingly similar to it.»

On April 25, a bill «On control over the activities of persons under foreign influence, » or rather, amendments to the legislation on «foreign agents, » was introduced to the State Duma. This draft law provides for the possibility of extrajudicial blocking of an information resource of a «foreign agent» in case of violation of the legislation on «foreign agents» (for example, for lack of labeling). The law also expanded the definition of this term, and hence the grounds on which Roskomnadzor can block the website of a person or organization recognized as a «foreign agent.» From this moment on, any person or structure (except for public authorities, state-owned companies and state corporations) can be considered a «foreign agent» if they not only receive foreign funding, but also are «under foreign influence» — with the widest possibilities for interpreting this definition. The first reading of the bill is scheduled for June 2022.

Who is punished

In 2012, when the first law on blocking was adopted, the main actors of the Internet were considered to be «hosting provider, » «site owner, » as well as «telecom operator» (the latter term was taken from the law «On Communications»: in Article 46 «Responsibilities of telecom operators» the Internet has been added to the traditional radio, telephone and television).

Organizers of information dissemination

- In 2014, the term «organizer of information dissemination» was introduced (97 FZ, Article 10.1). According to the law, it is.».*an entity carrying out activities to ensure the functioning of information systems and (or) programs for electronic computers that are intended and (or) used for receiving, transmitting, delivering and (or) processing electronic messages of Internet users.»* That is, an «organizer of information dissemination» is a website, platform, service or application that allows users to exchange messages or publish their own content.

According to the law, the «organizer» is obliged, firstly, to enter themselves in the appropriate register; secondly, to store information about the exchange of messages between users and information about users themselves for six months (this information should be stored only on the territory of the Russian Federation); thirdly, to provide this information to security and investigative agencies and keep the secret of the activities of these bodies.

- In 2016, the obligation to store the messages themselves was added to this list, as well as to provide the security and investigative agencies with means of decoding messages (374 FZ). The history of blocking of the Telegram app began with this point: Pavel Durov unsuccessfully tried to explain to the «authorities» that Telegram does not have access to encryption keys.

Hundreds of services and platforms that allow users to exchange messages and emails, publish their own information or even just comments, are in the register of «organizers of information dissemination, » which is maintained by Roskomnadzor. These can be both mail services and interactive maps, dating services, news sites, social networks, as well as any sites and applications if they allow the user to participate in the creation of content. In February 2022, the first 15 items of the register included the following «organizers of information dissemination»:

several services of Yandex, Rambler and Mail.ru, Odnoklassniki, VKontakte, ICQ, Habrahabr, the dating site mamba.ru, a news site with a comment feature «Roem», km.ru, www.liveinternet.ru, wikimapia.org, medianetworks.ru, a website about fire safety www.0-1.ru, the website «Moscow Tatar Free Word», etc. If the «organizer» refuses to enter the resource in the registry, access to it is restricted — it is blocked.

In April 2018, Article 10.1 became the reason for which the Zello app was blocked. It isa voice messenger that allows you to create thematic groups and which was used by truckers during protests against the introduction of the «Plato System» (a system for charging cars with a maximum permissible weight of over 12 tons). At the time of blocking, there were more than 14 thousand subscribers in the «Truckers» group (and in total about 400 thousand people used Zello in Russia, of which, according to RBC, about 100 thousand were in the «Debate» group, where they discussed politics and economics, and about the same number were in the «Religion and Politics» group). Roskomnadzor sent a request to Zello to register as an «organizer of information dissemination» within three days, threatening to block it. Inclusion in the registry automatically led to another requirement — according to the «Yarovaya Law», the «organizer of information dissemination» must store user data for a year and provide them at the request of law enforcement agencies along with encryption keys. However, voice messages are transmitted by Zello in real time and are not stored on the server for a long time. Zello developer Alexey Gavrilov (the company is registered and operates in Austin, Texas) commented on this requirement as follows: «*We would have signed up for the registry, but we can't store information about users in Russia... We only have 10% of users from Russia, and now we have to store everyone's data? This is nonsense.*»

The app was blocked, however, during 2017 and the spring of 2018, truckers continued to use Zello due to the block bypass technologies built into it in 2014. Then Roskomnadzor blocked the servers that were used by the app. Among the 36 blocked servers, 26 were owned by Amazon, which asked Zello to stop using its servers to bypass the blocks. The developers agreed, but a few months later Roskomnadzor discovered that Zello was now using Google's servers and blocked them. In a letter to the operators, as Meduza writes, Roskomnadzor reported that blocking subnets (in particular, Google servers) was an «experiment.» Such «experiments» took place for several years and were the result of the activities of a special department created by Roskomnadzor in 2017 to develop technologies for blocking prohibited Internet resources.

Search engine, news aggregator, owner of an audio-visual service, owner of a social network

- In 2015, the concepts of «search engine» and «search engine operator» (264 FZ) are introduced. Among other duties, the operator must, at the request of any citizen, remove access to «false information» (the so-called «right to be forgotten»).

- In 2016, the law introduced the concept of «news aggregator» (208 FZ). This is a Russian legal entity or a citizen of the Russian Federation who are «*owners of a computer program, owners of a website and (or) a website page on the Internet*» with the following conditions: these sites or pages publish information in Russian or the national languages of the Russian Federation and they have at least 1 million views per day. Like the «organizer of information dissemination, » the «news aggregator» is obliged to enter themselves in the appropriate register and store information about users for 6 months.

- In 2017, the law introduces the concept of «owner of an audiovisual service» (87 FZ) — a website, application, etc., which provides access to content «*for a fee and (or) subject to viewing advertising aimed at attracting the attention of consumers located on the territory of the Russian Federation.*» To have the right to distribute audiovisual content, the owner of the service must have an audience of more than 100 thousand users per day, talking only about those who are located on the territory of the Russian Federation. The owners of the audiovisual services also have their own registry and their responsibilities also include storing information about users for six months.

- Finally, in 2020, in addition to dozens of other amendments, the law «On Information» introduces the concept of «owner of a social network» (530 FZ). This is the owner of a website with 500 thousand or more users per day located on the territory of the Russian Federation. The «owners of social networks» also have their own registry and responsibilities, including not only storing information about users and their messages, but also compiling annual reports, and constantly monitoring the content of social networks.

- According to the draft law of 2022 «On control over the activities of persons under foreign influence, » information resources of «foreign agents» can also be blocked regardless of their type (website, social media account, etc.).

Defining state borders on the Internet

The explanatory note to the bill on the «sovereign Runet» begins with a mention of *«the aggressive nature of the US National Cybersecurity Strategy adopted in September 2018.»*

According to the explanatory note, the objectives of the new law are:

- «minimizing the transfer abroad of data exchanged between Russian users»;

- «control over cross-border communication lines and traffic exchange points»;

- introduction of a system of «centralized traffic management.»

To do this, the law provides for the installation of technical means which will make possible to restrict access to resources with banned information not only by network addresses, but also by prohibiting the passage of passing traffic. We are talking about communication lines that cross the state border of the Russian Federation: in these places, telecom operators are required to install «technical means of countering threats» (TMCT). Further orders and other documents clarify that we are talking about software for deep content filtering. According to the Roskomnadzor report for 2020, TMCT are installed on 100% of mobile devices and 50% of stationary ones.

The Law 90-FZ also introduced a new Article 14.2 of the law «On Information», which presupposes the creation of a «national domain name system.» The Roskomnadzor order issued a few months later identified the domain names included in the national system:

- domain names included in the top-level domain.RU;
- domain names included in the top-level domain.PФ;
- domain names included in the top-level domain.SU;
- domain names included in the top-level domain managed by a Russian legal entity.

In fact, we are talking about the nationalization of those Internet domain zones that have traditionally been Russian-speaking, although they were not under the direct control of the Russian Federation. The press wrote about the threat of full state control over the Coordination Center of National Domains back in 2016. Then, according to the journalists of the newspaper Kommersant, at a meeting in the Ministry of Communications with the participation of representatives of the FSB, the Ministry of Finance, the Federal Tax Service and Roskomnadzor, it was proposed «to de facto eliminate» the CC «in favor of the design formulated in the so-called bill on the «autonomous system of the Russian Internet.» That is, the actions of the Russian authorities in relation to the Internet have been logical and consistent, at least since 2016, given that the goal was isolation and control over the network.

THE SOVEREIGN RUNET

Vladimir Putin clearly stated for the first time that the Internet is «dangerous» for Russian society and needs state control in April 2014, during a media forum in St. Petersburg. According to the president, «the Internet emerged as a special project of the US CIA, and is developing in the same vein»; the press of that period wrote about the plans of the Russian authorities to strengthen the country's information security. In particular, regarding the placement of servers of large national Internet resources on the territory of Russia — this measure was presented as necessary, since «the Americans control the information flows» passing through their servers.

A couple of months before the media forum, the issue of control over the Internet was actively discussed in the State Duma and in the press: in February, amendments were made to the law «On Information» (adopted in April 2014 under the number 97 FZ), which equated bloggers with the media and obliged owners of Internet resources to store on the territory of Russia for six months information about users and the exchange of messages between them, as well as provide this information to security and investigative agencies. The accompanying amendments to the Code of Administrative Offenses provided for fines of up to 200 thousand rubles (for legal entities) for non-compliance with the requirements of this law. Large Russian IT companies, such as, for example, Mail.Ru Group, as well as human rights activists and experts criticized the new bill. The former pointed out that the implementation of the project would entail large financial losses, the latter claimed that the law could easily turn into an instrument of censorship.

One of the initiators of the bill, MP Irina Yarovaya, commented on it as follows:

«The organizers of the dissemination of information... will store information about the facts of the connection, but not the messages themselves. It is important to emphasize that bloggers are not required to store such information, since it is the prerogative of those who ensure the functioning of the information system or program. Thus, the norms of international law are not violated.» Law 97-FZ became part of the so-called «anti-terrorist package, » which also included laws expanding the powers of the FSB in the fight against terrorist threats and limiting non-personalized payments. Commenting on his initiative, Andrei Lugovoy mentioned the «events in Ukraine, » during which, according to him, «*all sorts of Western transfers for a penny inside the country merged into a multimillion-dollar stream of support for extremism and fired on the Maidan.*»

The following «anti-terrorist» laws, also initiated by Yarovaya in 2016, increased the storage period of information to one year and obliged site owners to store, in addition to information about the fact of messaging, also the content of these messages.

Thus, 2014 was the beginning of a large campaign to create a system of total control over the Russian segment of the Internet. To do this, the Russian authorities needed to develop ways to isolate this segment from the global Internet, which they understand as predominantly American. Three framework documents — the «Information Security Doctrine» (2016), the «Strategy for Countering Extremism» (2020) and the «National Security Strategy of Russia» (2021) — in combination with the laws «on the sovereign Runet» (2019) and «on landing» (2021) have created a legal basis for isolating the Russian segment of the network.

- «The Information Security Doctrine» appeared in December 2016 (the previous one was published in 2000). The main threats mentioned in it were: foreign intelligence services and the military; the technological lagging of the Russian Federation; terrorists; fraudsters; as well as two points that were not in the previous version of 2000 — discrimination of the Russian media in the West and «extremism.» Technically, the main danger, according to the doctrine, is the cross-border circulation of information — between users located on the territory of Russia and outside it.

- In «Strategy for Countering Extremism» (2020), the dissemination of information on the Internet, for example, calls for «unauthorized» rallies, is listed among the «most dangerous manifestations of extremism.»

- In «The National Security Strategy of Russia» (2021), special attention was paid to the issues of information security and the main factors threatening this security. According to the strategy, the Internet is an instrument of «interference in the internal affairs of the state» by foreign intelligence services, as well as control over information resources by transnational corporations. On the one hand, these corporations and states, «destructive forces abroad and within the country, » are engaged in «censorship and blocking of alternative Internet platforms, » that is, Russian media abroad. On the other hand, they «impose a distorted view of historical facts» and encroach on the foundations of the constitutional system of the Russian Federation, human and civil rights and freedoms, including by inspiring «color revolutions.»

The head of the Roskomsvoboda project, Artem Kozlyuk, in an interview for Novaya Gazeta, stressed that the «National Security Strategy of Russia» is an extension of the law «on the sovereign Runet»: «*So, the aggressive points of this strategy are not surprising and generally fall into the trend* *of the state towards aggression towards the Internet space and communications. Our state focuses its attention on the Internet not as an instrument of progress, creation, information exchange, but as an instrument of propaganda, politicization, dissemination of Western influence, etc.»*

The above-mentioned framework documents developed the concept of isolation of the Russian segment of the Internet — and at the same time new legislative initiatives introduced regular amendments to the laws «On Information», «On Communications», the Criminal Code and the Code of Administrative Offenses. In fact, in 2019, the law on the «sovereign Runet» (90-FZ) was adopted, in which the idea of American control over the Internet was reworked into the concept of the «sovereign Runet» — an isolated information system with special control over cross-border communication lines. And in 2021, the law «on landing» (236-FZ), or «On the activities of foreign persons in the Internet information and telecommunications network on the territory of the Russian Federation» was adopted, according to which all large foreign companies must open their offices in Russia under threat of blocking.

IT GIANTS

Throughout 2020, the Government of the Russian Federation, Roskomnadzor, the Ministry of Digital Development and other agencies have been developing rules and technologies for isolating the Russian segment of the Internet in accordance with Law 90-FZ. According to the experts of the Net Freedoms Project, «in 2020, regulatory support for the isolation of the Runet was generally completed, » since the government approved the rules for «centralized network management» and the regulations for the installation of TMCT (technical means of countering threats), and Roskomnadzor began to introduce them into the industry. Net Freedoms Project separately noted that «threats, in particular, include not only [the likelihood of] violation of confidentiality and integrity of communications, but also the possibility of access to information or resources prohibited in the country.» That is, the law formally adopted to create a stable system in case of «disconnecting Russia from the Internet» led to the development of a system for controlling or banning information, including blocking websites.

All this time, experts, activists and journalists wondered how the Russian authorities were going to influence the IT giants — Google, Facebook, Twitter, and other corporations whose owners and management were difficult to convince to follow Russian laws. In mid-2021, to solve this problem, the law «On the activities of foreign persons in the Internet information and telecommunications network on the territory of the Russian Federation» was adopted. The initiator of the law, Member of Parliament Alexander Khinshtein, calls it «the law on landing, » and experts of the Roskomsvoboda project — «the law on hostages.» The bottom line is that large foreign Internet corporations are obligated to open representative offices on the territory of the Russian Federation, which will be held liable before the Russian state — including for limiting the dissemination of banned information.

The law defines Internet corporations subject to new regulation as companies that:

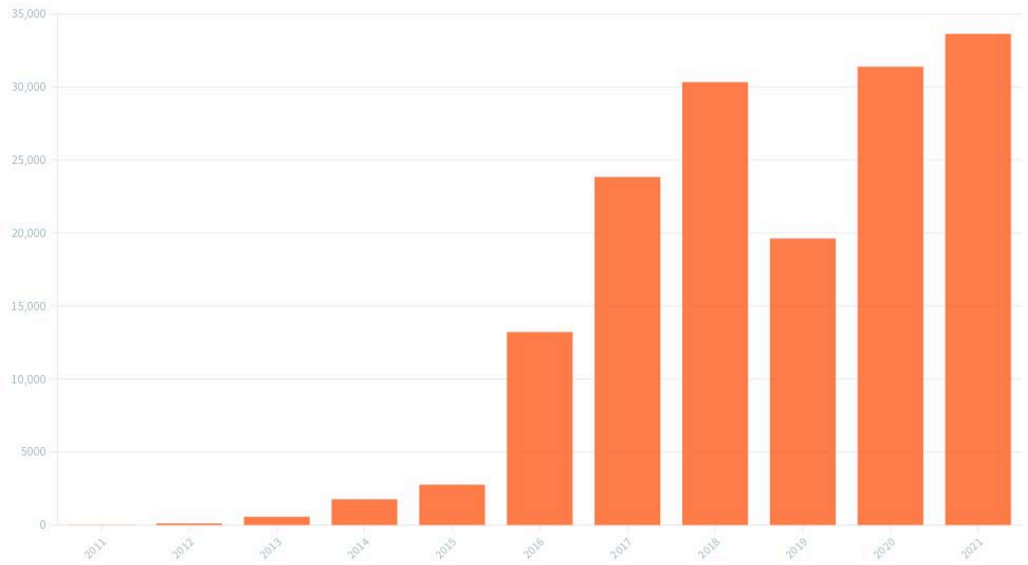
- were founded abroad by citizens of other countries;
- have at least 500 thousand users from Russia;
- distribute information in Russian or the official languages of Russian Federation subjects;
- distribute Russian-oriented advertising;
- process information about users from Russia;
- receive money from Russian citizens and legal entities.

The law stipulates the following measures of coercion in case of refusal of these companies to open a representative office in the Russian Federation:

- informing Russian users about violations of the law;
- prohibition on the transfer of Russian money to a foreign entity;
- a ban on the cross-border transfer of personal data of Russian users (Russians and Russian organizations will not have the right to transfer such data, so, in fact, it is a partial block);
- complete blocking on the territory of Russia.

In 2021 alone, foreign IT giants received fines of more than **9.4 billion** rubles for refusing to delete content and localize user data. Experts of the Net Freedoms Project in the report on the state of Internet freedom for 2021 (according to data for the first 9 months) listed foreign Internet companies that already got into the Unified Register: Youtube, Facebook, WhatsApp, Zoom, Telegram, Viber, Spotify, TikTok, Twitch, Pinterest, as well as Apple. «*This means*, » the report says, «*that each of the services is legally one step away from being slowed down or blocked, as happened with Twitter. Installation of Runet isolation equipment on communication networks (TMCT) already allows it*.»

Roskomnadzor blocks especially often content related to major opposition movements or organizations. For example, in January 2021, 12 materials on Youtube were blocked, «containing the same video with calls to participate in unauthorized rallies in January 2021.» Google LLC sued Roskomnadzor because there were no references to specific materials at all in the request of the Deputy Prosecutor General, but a video published in TikTok was mentioned. The Arbitration Court of Moscow dismissed the claim of Google LLC, ruling that the measures of Roskomnadzor were «prophylactic and preventive in nature.» In general, IT giants are trying to follow the new legislation — they meet with the Commission to investigate the facts of foreign interference in the internal affairs of Russia, pay fines, promise to remove banned information and apps (for example, in September 2021, Apple and Google LLC removed the Navalny app from their stores, and Google LLC also removed «smart voting» from the browser search results). In addition, Google LLC responds to requests from different states for the removal of certain materials and publishes data on these requests. In 2021, Russia was in first place in terms of the number of such requests (Turkey was in second place, followed by India and the USA). And according to the data for the period from 2002 to 2021, it is clearly visible how the appetites of the Russian authorities grew — especially in the column «Criticism of the government».



Requests of Russian Government to Google to Remove Content

Source: Google Transparency report

Made with Flourish • Create your own

On the other hand, Roskomnadzor controls the availability of official (and close to official) channels. The above-mentioned «censorship law» of 2020 was introduced to the State Duma the day after the Youtube channel «Solovyov LIVE» stopped appearing in the 'trends' section. Roskomnadzor accused Google LLC of «restricting the distribution of materials by a popular Russian author, preventing the growth of his audience.» In addition, Roskomnadzor sent a request to Google LLC about the reasons for the removal of Vladimir Putin's address from the NTV Youtube channel, a request to Twitter about the reasons for the absence of the RIA Novosti account in the search results, as well as general requests to several platforms at once, such as «stop censorship of Russian media» (RIA Novosti, RT, Sputnik and «Russia-1»). «*In the end*, » as the authors of the report «Internet Freedom 2020: the second wave of repression» (the Network Freedoms project) write, *«Roskomnadzor announced that it was a «purposeful policy by foreign platforms to influence Russians' access to objective information, » and recommended «Russian media and information resources to maintain the possibility* *of reliable and quick access to content by posting video materials on the platforms of Russian Internet companies*.» Simultaneously, Roskomnadzor initiated an administrative offense case against Google LLC and fined the company for 3 million rubles (this was the third fine).

After February 24, 2022, the situation for most IT giants has changed. Meta corporation has been declared extremist, and social networks Instagram and Facebook belonging to it have been blocked in Russia. Google and Youtube are still available, but they regularly receive threats from Roskomnadzor and from Member of Parliament who initiate most of the bills related to blocking.

HOW BLOCKS WORK

Banned information gets into the Unified Register in different ways. The blocking of sites associated with «undesirable organizations» occurs manually and is associated with other methods of repression aimed at the opposition or the media; that is, sites, pages and accounts of individual activists may be blocked not for content, but as a repressive measure. *«Some face administrative and criminal prosecution for the fact that they are actually activists, especially in regions where an investigator, prosecutor or employee of the Centre for Combating Extremism decided that they are too loud and it's time to charge them with something,»* said head of the Roskomsvoboda project Artem Kozlyuk at the OVD-Info round table.

In addition, according to the observations of Roskomsvoboda, many departments have a reporting system for the number of blocked resources. *«It makes sense to consider each category of banned information separately, »* says Kozlyuk. *«We have a dozen departments responsible for different pieces of censorship on the web, and they may have their own „ticking system" arranged differently. The tax service is now in the first place in terms of the number of blocks. This* *means that they may have a KPI for the number of resources blocked per month.»*

There are government agencies that respond to requests for blocking from users themselves, but, according to Roskomsvoboda, «pseudo-public organizations like the League for Safe Internet, cyber vigilantes, cyber Cossacks, cyber guards, » etc. are most often engaged in this. Moreover, a motivation system may exist within these organizations, for example, a «board of honor» with information about the number of complaints sent and the number of resources banned due to them —one, according to Kozlyuk, exists at the «Media Guard» (the project of the «Young Guard of United Russia»).

District prosecutor's offices, which report on the number of blocked materials, also have some kind of specialization. This new trend was noticed by legal analyst and head of the NetFreedoms Project Damir Gainutdinov: «*One district prosecutor's office specializes in electric fishing rods and illegal fishing gear, someone specializes in devices that help deceive electric meters, and someone — in the sale of alcohol*.» According to Gainutdinov, sometimes agencies overlap on topics — as in the case of online alcohol sales, where Rosalkogolregulirovanie (The Federal Service for Alcohol Market Regulation) competes with district prosecutors.

He also notes that in 2021, for the first time, the police initiated some of the blocks. We are talking about sites blocked in connection with cases of administrative offenses. «*Previously, everything was limited to the fact that a person was held liable, and now the Ministry of Internal Affairs also requests to block materials*, » Gainutdinov says.«*And prosecutors now report in their press releases: a person has been brought to criminal responsibility, and materials have been deleted or blocked.*»

In May 2022, after Russia's invasion of Ukraine, there were much more blocks with obvious political justification. Damir Gainutdinov adds: «Now I have a feeling that there is nothing but war... For example, there have been no non-war-related calls to our hotline in recent months. Previously, a dozen a week, at least: prohibited symbols, extremist materials, etc.» Despite this, according to his observations, «departmental blockages» continue, usually not directly related to political statements — for example, sites specializing in the illegal sale of alcohol or documents.

Finally, a noticeable (although small in percentage terms) number of blocks is the result of a direct political decision of the authorities. In such cases, all existing legislative norms are often used at once. Experts conditionally divide the blocks into 'mass' and 'targeted'. The first ones are rather «daily functioning» and are similar to «ordinary house cleaning» for the state, they have already become routine work and occur automatically. «*And there are, of course, politically motivated decisions*, » says Damir Gainutdinov, «*which are taken on the highest levels in relation to certain subjects, be they media or activists.*» Such blocks are separate cases, the result *of the* «order from above.» *«Then all laws are applied at once*, » explains the director and leading lawyer of the Mass Media Defence Center Galina Arapova. *«The organization is recognized as „undesirable" or „foreign agent" and all its content is cut out. The most striking example is the blocking of investigations of the „Project", „Team 29", FBK. They can be seen as exceptional, and they are clearly political in nature. Here, the whole complex of legislation was adjusted to a specific client, which allowed burning everything down to the ground.»*

Alexey Navalny's projects

In Russia, the largest number of blocks for various reasons, apparently, is connected to portals and publications related to Alexei Navalny and his projects. Over the years, his

LiveJournal, investigations, videos on YouTube channels, the Smart Voting project, etc. have been blocked. At the moment, in Russia access is blocked to the site navalny.com, the page of the Anti-Corruption Foundation (FBK), to all the sites of Navalny's regional offices, and the pages of some of the politician's associates.

LiveJournal: court decision, calls to participate in protests. Blocking the entire blog instead of individual pages

The first time the politician's team faced blocks was in 2014: Roskomnadzor blocked Navalny's personal page in Livejournal. The opposition politician's blog was included in the unified register of banned information at the request of the Prosecutor General's Office. The formal reason was that Navalny was then under house arrest as part of the investigation into the Yves Rocher case. It was impossible for a politician to use the Internet, but blog posts continued to appear — the texts were written on his behalf by Navalny's wife or his associates. *«The functioning of this Internet page violates the provisions of the court decision on the election of a preventive measure to a citizen against whom a criminal case has been initiated, »* Roskomnadzor said at the time.

However, it is not by chance that the first major blocks of portals related to the coverage of political events began in the same period: the sites of Grani.ru, Kasparov.ru and «Yezhednevnyy Zhurnal» were included in the Unified Register. At the same time, a copy of Navalny's blog, which was published on Echo of Moscow, was blocked — and the entire website of the radio station was unavailable for some time.

A few weeks later, the Prosecutor General's Office expressed its position, explaining the blocking of Navalny's blog differently — not by violating a court decision, but by calling for citizens to participate in «unauthorized mass events.» According to the law on information protection, the first ground — violation of a court decision — does not allow sites to be included in the register of banned information, while «calls» allow this to be done. Probably, the new public position of the Prosecutor General's Office was connected with this circumstance.

The agency explained that the «calls» appeared in an open group on VKontakte, which was called «The War against Corruption — support for Alexei Navalny.» From the photos and video materials posted in the group, it was allegedly «seen that during the events held, there was resistance to the legitimate demands of police officers.» The materials in the politician's blog, according to the Prosecutor General's Office, had a «single thematic focus» with such calls and formed «an opinion on the acceptability of the above actions.»

The group «War against Corruption — support for Alexei Navalny» was demanded to be blocked by United Russia's Alexander Sidyakin, and on March 13, the day Navalny's page was blocked in LJ, he received a response from the Prosecutor General's Office that this request would be satisfied. However, at the time of the release of the department's statement (April 2), the VKontakte group continued to open, but Navalny's blog did not.

A few months later, on July 28, the Moscow City Court rejected Navalny's complaint about the blocking. The court heard explanations of publications in connections with which the blog was blocked. Two entries were given as reasons: the first was dedicated to the events in Ukraine, but contained a call to come to support the defendants in the Bolotnaya Square case, and in the second readers were invited to come to court, where the verdict was to be announced in the same case.

Answering the question about the expediency of blocking the entire blog due to two entries, the Prosecutor General's Office stated that the law does not oblige it to specify particular blog pages when making a decision on blocking.

Roskomnadzor also explained that technically the blocking was carried out by the administration of LiveJournal, and they might not have been able to close access to individual blog entries.

Navalny deleted two specific entries that the Prosecutor General's Office referred to, but his blog in LiveJournal was unblocked only after a year and a half. According to the opposition politician, he did not understand why the block was not lifted, so at some point he decided to simply delete all the existing entries. After that, on November 11, 2015, the blog was unblocked, and the politician began to fill it in again. Simultaneously, Navalny's blog appeared on a new domain: navalny.com.

2018: blocks amid elections

The next round of pressure on Navalny and his team with the help of blocking occurred in 2018 and 2019, and, apparently, could be associated with the vigorous activity of the politician in connection with the presidential elections.

To understand the context of the blocks of these years, it is important to take into account that in 2016, Navalny announced his intention to participate in the presidential elections of 2018, after which he conducted a large-scale election campaign during 2017, which was accompanied by regular administrative arrests of a politician (or, for example, attacks by pro-government groups) and some of his associates. In the same year, mass protests «He Is Not Dimon to You» took place in Russia. However, at the end of 2017, the Central Election Commission refused to register Navalny as a candidate for the elections due to an outstanding criminal record in the Kirovles case. In response, the opposition politician launched a campaign calling for a boycott of the elections.

On February 15, 2018, after another rally organized by Navalny, the «Strike of Voters», at which he was detained, Roskomnadzor began blocking the politician's website navalny.com. The formal reason was Navalny's refusal to remove the FBK investigation dedicated to Vice President Sergei Prikhodko and businessman Oleg Deripaska from the site.

The investigation was published on the portal navalny.com on February 8, and the very next day, Roskomnadzor, by decision of the Ust-Labinsk District Court of the Krasnodar Territory, entered into the Unified Register of Prohibited Sites the address of the investigation on Navalny's website, its version on the YouTube channel and a number of news publications covering it. The court made the decision as part of the lawsuit of entrepreneur Oleg Deripaska against model Nastya Rybka (Anastasia Vashukevich) and writer Alex Leslie (Alexander Kirillov) for publishing materials about his personal life without permission: Navalny's investigation included data from open sources, including from the book and the Instagram account of Rybka, according to which the model was vacationing on a yacht in Norway in the company of Sergei Prikhodko and Deripaska himself.

As interim measures on the claim, the court ruled for the removal of the materials within three days, warning that otherwise the sites on which they are posted will be blocked. In addition, on the day the site navalny.com was blocked, Navalny was broadcasting on YouTube — immediately after the end, the platform blocked the recording, citing copyright infringement.

Navalny filed a lawsuit against Roskomnadzor in connection with the blocking, but it was not satisfied. Soon the politician's team removed the investigation from the site navalny.com, and after 5 days it was unblocked. «We believe that we resisted the blocking finely and the exercises were successful, » the opposition figure said, commenting on the decision to remove the material.

The «exercises» of Navalny's team came in handy really soon. In parallel with the campaign to boycott the presidential elections, the politician launched the Smart Voting project in early 2018 — his strategy aimed at the protest electorate was to reduce the number of victories of United Russia candidates in municipal elections scheduled for 2019. In December 2018, the project's website on domain 2019.vote was blocked by Roskomnadzor.

The head of the supervisory agency, Vadim Ampelonsky, said that the department had allegedly received complaints from several people that the site «illegally processes their data.» The formal reason was precisely this: according to Roskomnadzor, the privacy policy for processing personal data was not spelled out on the site.

Navalny filed a complaint about the blocking, and during its consideration, the opposition members explained that they do not work with personal data at all. However, representatives of the agency stated: information about users who did not register on the site was processed through Google Analytics and Yandex.Metrica services. At the same time, «the collected data was held on Google servers located in the USA» — from the point of view of Roskomnadzor, the site administrator in this case had to either provide the agency with a certified consent to the processing of personal data, or store the information on Russian servers. After blocking, the Smart Voting website moved to the domain appspot.com — a cloud platform supported by Google.

2021: recognition as extremist organizations, mass blocks

Against the background of Navalny's poisoning in August 2020, his return to Russia in 2021, the publication of the «Palace for Putin» investigation, the replacement of the politician's suspended sentence with a real one and the protests associated with all these events, the blocks again became an additional tool of pressure on the opposition politician and his associates. By the beginning of 2022, all sites affiliated with Navalny and his team had been blocked in Russia.

The blocks of 2021 can be divided into two streams: some were part of the process of combating Navalny's structures themselves and recognizing them as extremist organizations; others, apparently, served to deprive potential voters of access to the Smart Voting website.

Interestingly, the Smart Voting project was blocked even before the FBK and Navalny's regional offices were recognized as extremist organizations (this happened on June 9). For example, on May 6, YouTube sent out warnings to platform channel owners Vladimir Milov, Denis Styazhin and Ilya Yashin, as well as to Novaya Gazeta and SOTA media outlets about the prospect of blocking due to links to «Smart Voting», which the organization regarded as «spam, lies and fraud.» However, on the same day, the platform recognized the claims as erroneous, restored the deleted content and apologized to users.

By July 26, 2021, after Navalny's structures were recognized as extremist, almost all sites associated with them had been blocked. Among them is the website of the opposition figure himself, navalny.com, the pages of the FBK and Navalny's regional offices, the websites of his associates Leonid Volkov, Lyubov Sobol and Oleg Stepanov, the pages of the RosYama and RosZhKH projects, as well as the website of the Alliance of Doctors (which was not formally connected with Navalny in any way), and others. Leonid Volkov named the total number of blocked portals — 49 (according to Roskomsvoboda — 54).

Among the blocked resources were «mirrors» of the sites. As noted by Roskomsvoboda, this was, apparently, the first time that the mirror site (navalny.app) in Russia began to be blocked with the help of «technical means of countering threats» (TMCT). As experts noted, previously these technologies were used only to slow down Twitter. It is worth noting that navalny.app began to be blocked even before the appearance of Navalny's resources in the Unified Register of Prohibited Sites, which Internet service providers use to configure blocks. Mobile operators were the first to do this — at that time, all of them already had TMCT installed.

By July 26, 2021, the Smart Voting portal on appspot.com — Google domain — remained the only non-blocked resource associated with Navalny, although Roskomnadzor repeatedly tried to fix it. In fact, on June 23, the agency asked Google to stop technical support for the Smart Voting website, again naming violations of the rules for processing personal data as the reason. Kommersant managed to talk to Yekaterinburg lawyer Andrey Elantsev, who filed an official complaint with Roskomnadzor and formally initiated this process: he stated that the problem was storing user data on servers located in the United States. The same argument was also used by Roskomnadzor in 2018.

Nevertheless, for some reason, the portal was not blocked then — as Volkov later noted, this could be due to Google's refusal to meet the demands of the Russian authorities. On September 3 of the same year, the Moscow Arbitration Court banned Google and Yandex from showing the phrase «Smart Voting» in search results. This was done as an interim measure on the lawsuit of a little-known Stavropol company LLC Vulintertrade, which on July 27 — the day after the blocking of all Navalny's resources except Smart Voting — registered its rights to the trademark «Smart Voting». On September 6, the Smart Voting website was at last blocked, with the help of the TMCT. Roskomnadzor explained this decision by the fact that the site was allegedly «used to continue the activities and events of an extremist organization.» At that time, Smart Voting mobile apps and a Telegram bot were still available, but by the elections (September 17-19), they also became inaccessible.

On September 17, the Navalny app with the Smart Voting function was removed from the Russian Google and Apple stores (they remained available in stores in other countries). Roskomnadzor has been demanding this since mid-August and threatened companies with fines in case of disobedience. The New York Times claimed that Google agreed to remove the Navalny app from the Google Play store after threats of criminal prosecution of company employees.

On September 18, the «Smart Voting» bot in Telegram was unavailable for some time. Then the owner of the application Pavel Durov explained the situation with a «day of silence» and a ban on election campaigning during the vote, but later said that the work of the bot was suspended due to the threat of a block of the entire Telegram app in Russia.

Open Russia

Like Navalny's structures, projects related to Mikhail Khodorkovsky have repeatedly faced blocks. Unlike Navalny's resources, however, most of the blocking of sites supported by Khodorkovsky was justified by a single reason: interaction with an undesirable organization.

Khodorkovsky's resources were massively blocked for the first time in 2017 on the basis of the law on «undesirable organizations» adopted two years earlier — foreign and international structures that «pose a threat to the foundations of the constitutional system, the defense capability and security of the state.» In April 2017, the Prosecutor General's Office recognized the British structures Open Russia Civic Movement and Otkrytaya Rossia as undesirable. And although their connection with the Russian movement «Open Russia», which Khodorkovsky supported, is very doubtful, the new status became a formal reason for the persecution of the movement and its members by various methods, including through blocks.

On December 12, 2017, Roskomnadzor blocked the Open Russia website (openrussia.org) at the request of the Prosecutor General's Office, as well as a number of other portals related to Khodorkovsky: «Instead of Putin», «Khodorkovsky.ru», «Open Law», «Open Russia Team» and «Open University». The Roskomnadzor website said that the Open Russia website was added to the register of prohibited sites on December 11 on the basis of Article 15.3 «On Information, Information Technology and Information Protection.» The article allows to block resources that, according to the Russian authorities, contain «calls for mass riots and extremism» and «information materials» of organizations whose activities are recognized as «undesirable» on the territory of Russia.

Later, both the Prosecutor General's Office and Roskomnadzor issued statements confirming that Khodorkovsky's resources were blocked for distributing materials from «undesirable» organizations. At the same time, as the then editor of the Open Russia portal Veronika Kutsyllo noted, the editorial office received a warning about the blocking on December 11 only about the site old.openrussia.org — a resource where old materials published before 2016 were stored. Specific details about the connection of the site materials with Article 15.3 of the Federal Law «On Information» were not given to the owners; there were no indications that other resources of the movements were under a threat of blocking.

Some social networks, such as YouTube and Twitter, have also received the requests to block Open Russia accounts. Roskomnadzor even threatened the YouTube video hosting with a complete block if it refused to delete the Open Russia channel.

After blocking, the site moved to a backup copy (open-russia.org), for some time the portal changed the «mirrors», but in the end the project was closed, and the team created a new media, MBH Media. It was not registered as a media outlet and belonged personally to Mikhail Khodorkovsky. Khodorkovsky commented: *«We made such a decision, because according to the new „law", a legal dispute about the cancellation of the blocking of the site can go on for almost a year, and I will switch to other forms of information confrontation if all possible methods provided for by „their" laws are exhausted.»* And the editor-in-chief of the site Veronika Kutsyllo said that during the last nine days before the «move» to MBH Media, the project had to change the «mirrors» more than 20 times — all of them were blocked in turn.

Two months later, on February 21, 2018, the MBH Media website was also blocked by Roskomnadzor. It happened again at the request of the Prosecutor General's Office, on the basis of the same Article 15.3 of the Federal Law «On Information, » only this time the journalists did not receive any notifications about the upcoming blocking. After that, the MBH Media website moved to the Google domain appspot.com, and existed there for some time without blocks.

A new wave of repression on the Internet affected Khodorkovsky's projects in 2021. On August 4, the websites of two media projects of the oligarch, Open Media and MBH Media, were blocked according to the same scheme: the Prosecutor General's Office's demand on the basis of Article 15.3 of the Federal Law «On Information, » more specifically — for publishing «information materials» of «undesirable» organizations. In addition, the order of Roskomnadzor extended to another human rights project of Khodorkovsky — «Pravozashita Otkrytky.» The next day, MBH Media and Open Media announced the closure, and Pravozashita Otkrytky deleted all entries in its Telegram channel. The next day, Roskomnadzor blocked website of the «Profession is Journalist» award, also established by Khodorkovsky.

Commenting on the decision to close, all three projects — «MBH Media», «Open Media» and Pravozashita Otkrytky — referred to the risks that communication with «undesirable» organizations, in the form that the Prosecutor General's Office understood, carried for members of editorial offices and other project participants. Considering that these projects have been working without such restrictions for three years, it can be concluded that the blocks served as a signal to the members of the newsrooms about potential repressions.

BLOCKS AFTER FEBRUARY 24, 2022

Blocks and self-closure of media outlets

Immediately after Russia's invasion of Ukraine, on February 24, Roskomnadzor informed the media that they should use only official information when covering the «special operation.» For non-compliance, the agency threatened them with fines under Article 13.15 of the Code of Administrative Offenses and blocking under Article 15.3 of the law «On Information». This document, according to Damir Gainutdinov, meant radical changes in law enforcement: «*What has fundamentally changed is the approach to assessing the reliability of information. The press release of Roskomnadzor dated February 24 says that everything that is not confirmed by official Russian sources — and these are state authorities and state media — is all fake. And this is evident from the notifications of Roskomnadzor, which refer to the requirements of the Prosecutor General's Office. The only argument for the unreliability of the information is that the Ministry of Defense does not confirm it… On this basis, a request is issued to Roskomnadzor, which sends it to the media, and by default everything is blocked. Moreover, if in the early days these requests were related to specific publications, then later they began to indicate not the page address, but the domain name of the site.*»

On February 26, Roskomnadzor published news about the frequent cases of the dissemination of «false information» with the threat to restrict access to materials of **Echo of Moscow**, **InoSMI**, **Mediazona**, **The New Times**, **Dozhd TV channel**, **Free Press**, **Crimea.Realities**, **Novaya Gazeta**, **Journalist**, **Lenizdat**», and **Wikipedia** (for the article «Russia's Invasion of Ukraine») According to the wording of the agency, on these resources, «*under the guise of reliable messages, socially significant information is posted that does not correspond to reality about the shelling of Ukrainian cities and the death of civilians in Ukraine as a result of the actions of the Russian Army, as well as materials in which the operation is called an attack, invasion, or declaration of war.*»

On February 28, the following were blocked: «**The Current Time**» (from a letter from Roskomnadzor: «*False socially significant information about the Russian military allegedly killed and captured on the territory of Ukraine during a special military operation conducted by the Armed Forces of the Russian Federation*»), the website **Crimea. Realities** (Radio Liberty), the student magazine **Doxa** (a few hours before the blocking, the agency demanded to delete the article «Handbook for anti-war disputes in the family and at work»),**The New Times** (for an article on the federalization of Russia). On the same day, Roskomnadzor demanded from the TikTok administration to *exclude from the recommendations for minors any military or political content*.

On March 1, the websites of two media outlets were blocked at once, which soon ceased their activities — radio station **Echo of Moscow** and the TV channel **Dozhd**. The reason was «*purposeful and systematic publication of deliberately false information about the actions of the Russian military in the framework of a special operation to protect the DNR and LNR*.» On March 2, the newsroom of Dozhd TV channel ceased its activities, and on March 2, the board of directors of Echo decided to liquidate the radio station and the website by deleting their accounts in social networks.

From March 1 to March 6, with various justifications («calls to extremism», «false socially significant information», including «life-threatening», etc.), websites of **Taiga.Info** (for more information about this case, see the chapter «Legislation on blocking»), **The Village** (closed the office in Moscow and continued working from Warsaw)**, Tomsk TB2 Agency** (suspended the work), **Znak.com** (suspended the work), **Mediazona** (continues to work) and **Meduza** (continues to work), were also blocked. At the time of writing, only two cases of unblocking are known: website of the Snob magazine (the editorial board deleted all materials about the war in Ukraine and refused to cover this topic), as well as Novye Izvestia. After two warnings from Roskomnadzor, Novaya Gazeta, which received the Nobel Peace Prize last year, announced that it was deleting all its materials about the war in Ukraine for the safety of journalists, and on March 28 suspended publication «until the end of hostilities.» After the forced departure of some journalists of the outlet due to pressure from the authorities, they announced the launch of a new project «Novaya Gazeta. Europe». This happened on April 7, and the project was blocked in Russia already on April 29.

We can say that by the beginning of March 2022, the Russian information field was almost completely under the control of the state.

It should be noted that Roskomnadzor provided the request of the Prosecutor General's Office dated February 24, on the basis of which a decision was made to block Meduza, only on May 20 — at the court trial where it was considered. The document lists the publications of eight media outlets from Russia, Kazakhstan, Georgia, Armenia, and Estonia, which, according to the agency, contain «untrue information, » namely, «materials about the alleged attack by Russia on the territory of Ukraine.» However, the document does not mention the publications of Meduza and there are no references to this outlet, but it contains the following wording: «In case of reproduction of similar materials on other Internet resources, I also demand to restrict access to them.» Such information, according to the prosecutor's office, «creates panic moods in people, creates prerequisites for a massive violation of public order and public safety.» In reality, this is a carte blanche for lightning-fast blocking of any «unwanted» resources.

Earlier, the Prosecutor General's Office refused to show this document, stating that it «contains information, the disclosure of which may entail a violation of the rights of third parties.»

Blocking of foreign media

Also in early March, many foreign media broadcasting in Russian and to a Russian audience were blocked: **Voice of America**, **BBC Russian Service**, **Deutsche Welle**, **Radio Liberty** (these may include **Meduza**, formally located in Latvia). Roskomnadzor explained their blocking by the spread of «fakes about Ukraine.» The BBC Russian Service, as well as Bloomberg and CNN announced the suspension of work in Russia, Meduza continues to work.

On March 21, Euronews TV channel was disconnected from the air; the next day, the broadcasting of the state channel Russia 24 was launched on their frequency, and on April 7, a new TV channel Solovyov.Live by journalist Vladimir Solovyov (included in the EU sanctions lists for supporting Russia's hostile actions against Ukraine) began broadcasting instead.

Blocking major media platforms

Most of the IT giants, despite their loyal behavior towards the Russian authorities in the past, reacted to the invasion of Ukraine unequivocally negatively. In fact, already on February 24, **Meta Platforms, Inc.,** which owns the social networks Facebook and Instagram, has restricted the official accounts of the Zvezda TV channel, the RIA Novosti news agency, and the Lenta.ru and Gazeta.ru platforms. In addition, the company imposed restrictions on the search output of materials from some Russian media, began to label them as unreliable and marked them with a label about them being under control of Russian state structures. The next day, on February 25, the Prosecutor General's Office, in coordination with the Foreign Ministry, recognized Meta as «involved in the violation of fundamental human rights and freedoms, as well as the rights and freedoms of Russian citizens» and slowed down the traffic of Facebook and Instagram networks. Facebook was completely blocked in Russia on March 4, on the «night of the blocks»; on March 14, the same thing happened with Instagram; and on March 21, the entire Meta company was recognized as extremist.

On March 1, Roskomnadzor started slowing down **Twitter** again (like most other foreign platforms, based on Law No. 272-FZ*«On measures to influence persons involved in violations of fundamental human rights and freedoms, the rights and freedoms of citizens of the Russian Federation»*, or «on censorship»), and on March 4, blocked the social network completely.

On March 6, the Zello application was blocked — after *«demands to stop sending messages to users that contain false information about the course of a special operation of the Armed Forces of the Russian Federation on the territory of Ukraine.»*

Among the major social networks that can be freely used on the territory of Russia, there are now only**Telegram** (RKN only demanded from the company to delete accounts from which Russian soldiers receive requests for information about their whereabouts) and **VKontakte** (before blocking Instagram, Roskomnadzor recommended that users switch to Russian networks as soon as possible, including VKontakte) left.

Unlike many IT giants, **Google**'s services are still not blocked in Russia. At the same time, Google constantly receives threats from Roskomnadzor, pays heavy fines and takes its employees out of the country.

On March 1, **Google** blocked RT and Sputnik Youtube channels in Europe due to Russia's invasion of Ukraine, and then Youtube suspended monetization functions in Russia. That is, you can use Youtube on the territory of Russia, but you cannot earn money with it. On March 10, the **Google Pay payment system became unavailable in Russia.** On the part of Russia, only one service was blocked — **Google News**, but «coercive measures of an informative and economic nature» were introduced *against the company.* Roskomnadzor issued a ban on the advertising of Google LLC, and the other search engines, in particular, Yandex, are now required to label links to Google sites with the following: «*Roskomnadzor has decided to inform users of ****** that a foreign person who owns information resources is a violator of the legislation of the Russian Federation*.»

Nevertheless, Google and its services continued to block official websites and channels in Russia. In fact, on April 9, **YouTube** blocked the official channel of the State Duma — as explained by Google, «in accordance with the sanctions against Russia.» According to Artem Kozlyuk, co-founder of the Roskomsvoboda project, blocking Youtube in Russia is a matter of time. However, at the time of writing, neither Google nor Youtube were blocked in Russia.

In addition to Russian and foreign media, the websites of human rights organizations (Golos, the movement For Human Rights and Amnesty International), as well as individual pages of opposition politicians who opposed the war (Mikhail Khodorkovsky, Alexei Navalny and the pages of Navalny's team, Ilya Yashin, Ekaterina Shulman's fan group, and others) were blocked.

Also, on May 30, Roskomnadzor, at the request of the Prosecutor General's Office, blocked the website of the Memorial Human Rights Center. It is obvious that the trend will only continue — especially after the entry into force of the law on «mirror blocks» — until the space of the Russian-language Internet is completely cleaned up.

TECHNOLOGIES

The «Revisor» system

Since 2012, when amendments to the law «On the Protection of Children» introduced a Unified register, telecom operators were obliged to block Internet resources entered there by Roskomnadzor. At first, the agency's inspectors controlled the operators manually, but since the end of 2015, Roskomnadzor has begun to implement the «Revisor» system, which automatically checks whether the operator blocks prohibited sites. As the RBC newspaper explained, «if the system detects that the operator provides access to more than 1% of the resources from the register of sites with illegal content, it sends a notification about it to Roskomnadzor.» Since December 1, 2016, Roskomnadzor has obliged all Russian telecom operators to connect to the «Revisor.»

The «Revisor» system only records violations, but cannot be a tool for blocking sites. For this purpose, after the adoption of the law «on the sovereign Runet», TMCT, or «technical means of countering threats» were introduced.

TMCT, or deep packet inspection (DPI)

TMCT is a broad concept, which can include a variety of hard — and software. According to the newspaper Kommersant, after the adoption of the law, the Ministry of Communications explained that DPI equipment (Deep Packet Inspection, deep traffic filtering), among other things, belongs to the TMCT. It is the prerogative of Roskomnadzor to determine which specific system telecom operators are required to install.

DPI's task is to filter traffic and restrict access to banned sites.

Analysts at the Carnegie Moscow Center believe that the idea of using DPI belongs to Sergey Kiriyenko, who is «the real author and ideologue of the law on the sovereign Runet.» According to them, it is Kiriyenko who is responsible in the presidential administration for «the Internet and everything connected with it»; he made serious efforts to ensure that the law on the sovereign Runet was adopted, including achieving a change in the position of the Ministry of Communications (at first, representatives of the Ministry of Communications were categorically opposed, but then supported the bill). Before the law on the introduction of the TMCT, these technologies were used by large corporations in order to limit the ability of their employees to use social networks and other resources not related to their duties during working hours. In addition, DPI is one of the Internet censorship technologies that China uses at the national level.

According to an unnamed representative of Roskomnadzor, quoted by RBC, by the beginning of April 2020, «100% of mobile traffic and almost 60% of broadband fixed traffic passes through the TMCT equipment, » that is, about 80% of operators have installed these systems. In May 2021, the head of Roskomnadzor, Andrey Lipov, in an interview with the Kommersant newspaper, said that more than 421 million attempts to access «banned information» had already been prevented with the help of TMCT.

Two years before the entry into force of the law on the «sovereign Runet», Roskomnadzor tested EcoFilter equipment manufactured by the company RDP.ru (owned by Rostelecom) as a TMCT on the networks of the Ural Federal District. The authors of the resource Habr.com believe that it is these devices that are mainly installed in Russia as the TMCT. «*This system*, » they write, *«analyzes all Internet traffic (packets) of users by a number of parameters and decides whether to let it pass (by default), limit the speed (rules for Twitter and possibly Google), or block it (for banned sites). Only RKN specialists set up and manage the TMCT elements.»*

At the same time, experts agree that it is technically impossible to install a TMCT on 100% of the Internet, since the outlines of the network change all the time. They also believe that this technology does not protect against external threats in any way, and the «sovereign Runet», as Mikhail Klimarev, director of the Internet Protection Society, comments to the RBC website, is created exclusively «for censorship, suppression of dissent, and economic pressure on Internet corporations.» Experts also noted that TMCT is a very expensive technology, and its mass use, moreover, can lead to large outages in networks. In fact, the CEO of the provider Diphost, Philip Kulin, comments for RBC: «The cost will be cosmic, and with abnormal loads, various delays may still occur. I claim that no one can afford to analyze absolutely all the passing traffic right now.»

Unlike SORM-2 and SORM-3, DPI technologies allow one to actually cut off prohibited resources from the network managed by the telecom operator. At the same time, the system can distinguish a traffic packet of one platform or application from others (for example, Telegram from Facebook), but does not see the contents of this packet. As the experts of the Roskomsvoboda project write, «it is impossible to read the contents of encrypted packets, but you can understand from the metadata which sites the user is looking at, and, in most cases, which data exchange protocol he uses.»

One of the first experiences of using the TMCT in Russia was the slowdown of Twitter in March 2021 (a detailed analysis of the technologies is given in the report of Censored Planet «Throttling of Twitter in Russia». Roskomnadzor openly commented on these measures as «testing» the system. The slowdown has caused major disruptions to other services and platforms, including government websites. In July 2021, Roskomnadzor also blocked the websites of Alexei Navalny and his team using DPI. According to experts, this was the first domain lock using the TMCT.

Artificial intelligence, automated systems, and content analysis

In order to identify prohibited content en masse, Roskomnadzor and other agencies have been ordering and buying automatic search systems for keywords, images, video, and audio for several years. Andrey Lipatov, the head of Roskomnadzor, told about the use of «neural networks and projects related to artificial intelligence» to improve the effectiveness of monitoring publications in social networks and services in an interview with Kommersant newspaper in May 2021: «*Obviously, when it comes to billions of messages, it is impossible to make decisions manually. After the initial monitoring, only a part of the messages will be received by operators. Now we predict that by the end of the year, the amount of information that our employees will be able to analyze will increase by 14 times. The decision to block is made by authorized employees, after which the data is transmitted in the format of a register to telecom operators.*» Lipatov also explained that the agency creates a significant part of the projects independently — a scientific council was created on the basis of the GRCC (Main Radio Frequency Center), to which «the leading players of the Russian market in the field of artificial intelligence were invited.» The rest is ordered from third-party developers. «*We are trying to make a modular system,*» says Lipatov, *«To make it easier to develop, to use different subsystems for different purposes. We order some cubes from Russian developers, because it's faster and more reliable: they always provide us with the proper level of support.»*

According to Stanislav Seleznev, an expert of the Net Freedoms Project project, «*given the number of materials that are blocked by each department, this is happening more and more often in an automated mode.*» For this purpose, autonomous information systems are used, such as AIS «Search», which catch materials by keywords or images. «*There is software related to the analysis of video and audio in different services,*» says Seleznev. «*If you look at public procurement or registers of software approved for use by public services, there will be many systems for searching for prohibited content. Those same „cyber-cossacks“ are now less likely to scroll the feed of some opposition figure, because they have a system with a user-friendly interface into which they upload the words they thought about. There is competition among IT developers working for and in the interests of prohibiting the dissemination of information, to search for prohibited content.*»

Another system known to specialists — «Laplace's Demon» — was created not by an order of the authorities, but on the initiative of its developer, the founder of the NGO «Center for the Study of Legitimacy and Political Protest» Evgeny Venediktov. According to him, it differs from conventional keyword search systems and can analyze not only individual posts, but also mark «protest moods» in general. Until 2017, the Center was still waiting for potential customers, among whom, according to Venediktov, there should have been not only scientists, but also government agencies, including law enforcement agencies, and conducted its own monitoring, though not of all traffic, but of its individual groups. As Venediktov said in an interview with the Izvestia newspaper, «three types of groups will be monitored: politically oriented, social protest groups, and local discussion platforms that unite users on a geographical basis.» According to the press, by 2018 Venediktov became a contractor for the Ministry of Internal Affairs.

For 2020-2021, according to the Roskomsvoboda report on public procurement for the purposes of

surveillance and behaviour monitoring, at least **5.6 billion** rubles were spent on tenders, of which at least **620 million** rubles were spent on purchases related to the monitoring of social networks and the media, and another **580 million** rubles were spent specifically on the development of monitoring and tracking systems for the Ministry of Internal Affairs, Roskomnadzor, the Centre for Combating Extremism, and other agencies.

Blocking access to VPN

The legal basis for blocking VPN services was laid down by Law 276-FZ, which obliges VPN service providers to connect to the federal state information system (FGIS), which is under the jurisdiction of Roskomnadzor. The system contains a list of prohibited resources that the VPN service should also block. According to the Roskomsvoboda project, in 2019, the services refused to register in the system.

In 2021, after the introduction of the TMCT system subordinate to Roskomnadzor, the technical possibility of blocking VPN services appeared. In June 2021, for the first time, the use of individual VPN services was banned on the basis of their refusal to register. As a result, OperaVPN (browser extension) left Russia, and Google agreed to remove hundreds of thousands of links to other VPN services from the output. The first attempt to restrict access to VPN occurred in September 2021 — on the eve of the State Duma elections and after blocking (with the help of the TMCT) resources associated with Navalny. Since then, Roskomnadzor has regularly blocked VPN services, as well as VPN protocols (which is why other services suffer — for example, streaming videos, online games, etc.). Roskomsvoboda experts believe that it will be impossible to completely block access to the VPN, but it will take a lot of «manual labor» to bypass the blocks. Probably, with further blocking, only professional IT workers will be able to freely use «prohibited» Internet resources.

After February 24, 2022, when the socio-political media began to be widely blocked, VPN services and anonymizers became the only way to access information. According to the calculations of the mobile operator Yota, since the beginning of the year, the number of users of VPN services in Russia has increased 53.5 times. In February and March, VPN applications accounted for 8 out of 10 downloads in the Russian App Store.

Despite the sharply increased popularity of VPN, a large number of Internet users in Russia do not have access to information after mass blocks. It can be assumed that this is a more conservative part of the audience, and an alternative news picture remains inaccessible to it. Taking into account the growing self-censorship service «Yandex. News», which has been putting more than 70% of links to state-related media since the beginning of the war, there are practically no available sources of non-state news.

At the end of May 2022, Roskomsvoboda signed an open letter to a large non-profit organization for the protection of digital rights, Access Now, in which it urged not to impose sanctions against Russia and Belarus on software, equipment, technologies and services related to the exchange of information via the Internet. According to activists and human rights defenders, «sanctions will only accelerate the offensive of the „sovereign Runet“, » since they only strengthen the state’s position on restricting access to information. A similar letter addressed to US President Joe Biden was also signed by 35 human rights organizations from different countries, including Russia and Belarus.

Global platforms have also though about access to information for residents of Russia. In fact, Twitter together with Tor have developed a blocking bypass technology, and Windscribe has tripled its bandwidth and provides users in Russia with free access, since they are unable to pay for the service. In addition, they also provided the Russians with promo codes «PEACE» and «pizdets, «which can be used to get 30 gigabytes per month. ProtonVPN offers a free subscription for Russians, Belarusians and Ukrainians — to do this, you need to write to the technical support of the service.

BLOCKING AND CIVIL LIBERTIES

Freedom of expression in the context of blocks

The Internet provides an unprecedented platform for the exercise of freedom of expression. Given its accessibility and the ability to store and transmit huge amounts of information, the Internet plays an important role as a tool for increasing public access to news and facilitating the dissemination of information in general.

The human right to freedom of expression, including online expression, is enshrined in Article 10 of the European Convention and Article 19 of the International Covenant on Civil and Political Rights. Despite the fact that this right is not absolute, it can be restricted only if the following conditions are strictly observed: the restriction of the right must 1) be based on a foreseeable law, 2) pursue a legitimate aim, and 3) be necessary in a democratic society, proportional.

As a general rule, if an opinion is related to issues of public interest and contains criticism of public policy and public figures, it is subject to the greatest degree of protection, and the state must have fewer legal ways to restrict the expression of this opinion. Thus, the European Court of Human Rights pointed out that political journalism may even include «some degree of exaggeration or even provocation.» The UN Human Rights Committee and the Special Rapporteurs stressed that blocking online media or websites because they criticize the government or the political system cannot be considered a necessary restriction on freedom of expression.

In 2011, four representatives of intergovernmental bodies for the protection of freedom of the media and expression (UN, OSCE, Organization of American States, and the African Commission on Human and Peoples' Rights) issued a joint Declaration on Freedom of Expression and the Internet. Section 3 «Filtering and blocking» stipulates that the forced blocking of Internet resources at any level — from a single page to a protocol — is an extreme measure that can be justified «*in accordance with international standards, for example where necessary to protect children against sexual abuse*» (p. 88).

The UN Human Rights Council has also condemned the use of Internet blackouts by states to deliberately and arbitrarily prevent access to information. The Council also called on States to refrain from censorship and blocking of publications and media outlets.

In May 2022, the UN, the African Commission on Human Rights, the Inter-American Commission on Human Rights, and the Organization for Security and Co-operation in Europe stated that even disinformation cannot be combated by blocking or banning the media. Any restriction on freedom of expression must strictly comply with three criteria — legality, legitimate aim, necessity and proportionality.

In turn, the European Court in its practice, which includes several cases against Russia, has developed the basic principles states should be guided by in the issue of blocking information on the Internet.

Firstly, despite the fact that blocking websites or publications on the Internet is not illegal itself, blocking can only be carried out in accordance with foreseeable national law that would clearly indicate which information is prohibited and can be blocked. Authors of publications should be able to understand clearly what information they can distribute and what they cannot.

Secondly, in order for the restriction of information to pursue a legitimate aim and be proportional, the blocking must be selective, narrowly focused. Indiscriminate blocking is prohibited. This means that only specific content that is prohibited can be blocked, blocking the entire resource due to a single publication is not allowed, since this would lead to excessive collateral damage. Indiscriminate blocks are arbitrary blocks.

In this regard, the European Court ruled in several cases that the complete blocking of a website is an **extreme** measure, which, according to the UN Human Rights Committee and other international bodies, is equivalent to the complete closure of a print publishing house.

Thirdly, the author of the information must have procedural guarantees that do not allow abuse of her/his rights. In particular, the author of the information should be notified about the blocking of the content, indicating the reasons for the blocking. The author must be given a choice: delete the information or leave it, otherwise their right to freedom of expression will be violated. In addition, the author should be able to present in court their arguments regarding the legality of the information he distributes **before** blocking. It is the court that can properly assess whether the restriction of the right to freedom of expression is necessary and proportionate, and whether alternative and less restrictive measures were available to achieve a legitimate goal.

Moreover, The European Commission for Democracy through Law (Venice Commission), whose findings are taken into account by the European Court of Justice, stressed that the temporary cessation of media activities is possible only in case of repeated publication of information that is not only illegal, but also directly calls for unlawful violence against individuals or groups, for the violent overthrow of the constitutional order. The Venice Commission also noted that the decision on blocking should be taken by the court, not the administrative authorities.

The European Court has repeatedly analyzed the Russian legislation on blocking and concluded that it does not comply with international standards. For example, in 2020, the European Court considered 4 cases in one day, in all cases recognizing that the blocks violated the applicants' rights to freedom of expression.

In the case «Vladimir Kharitonov v. Russia», it was found that Article 15.1 of the Law on Information allows the authorities to block the entire website without distinguishing between legal and illegal content. The provision of the law granting the executive body such a wide freedom of action carries the risk of arbitrary and excessive blocking of information. The European Court found that the blocking of the applicant's website on the basis of this article violated his right to freedom of expression.

In the case «Engels v. Russia», concerning the blocking of the page of the Roskomsvoboda website, the European Court concluded that subparagraph 2 of part 5 of Article 15.1 of the Law on Information, which allows blocking «prohibited» information by a court decision, does not meet the criteria of a «quality» of law. The Court noted that the vague and excessively broad wording of the provision did not satisfy the requirement of foreseeability of the law. This rule does not give website owners the opportunity to regulate their behavior, since they cannot know in advance what content may be called prohibited, which will lead to the blocking of their entire website. In addition, the court considered that it is impossible to prohibit content-neutral information dissemination technologies, such as VPN, only on the grounds that they can theoretically be used to gain access to banned information.

In the case of Bulgakov v. Russia, the European Court found that part 6 of Article 10 of the Law on Information, which allows blocking information for the dissemination of which criminal or administrative responsibility is provided, does not actually provide for the possibility of blocking the entire site due to separate «prohibited» content. Because of this, the blocking of the applicant's entire website on the basis of this rule was not legal. In addition, the European Court added that, in violation of international standards, this law does not provide for the requirement of communication of a decision to the author of «prohibited» content.

Finally, the case of Flavus and Others v. Russia considered the issue of the blocks against Grani.ru and Yezhednevnyy Zhurnal, which published information about the Bolotnaya Square case, and the website Kasparov.ru, which posted a publication about the Crimea. The European Court found that the wording of part 1 of Article 15.3 of the Law on Information, which allows for **the extrajudicial** blocking of information containing calls to participate in «mass (public) events held in violation of the established procedure, " is too broad and vague. It allows the Prosecutor General to make a decision to block information about an event committed in case of any violation of the procedure of its conduct, no matter how insignificant or harmless it may be, without establishing the risk of serious riots or any real violation of the rights of others. In addition, this law does not require the authorities to assess the impact of blocking measures on freedom of expression before their implementation or to justify the urgency of their immediate application, not giving interested parties an opportunity to remove illegal content or go to court before the immediate blocking.

Article 15.3 does not provide the owners of online media with any procedural guarantees capable of protecting them from arbitrary interference by the authorities. It does not require any form of participation of site owners in the blocking procedure. The Court also noted that the Law on Information does not require the authorities to justify the necessity and proportionality of interference with freedom of expression on the Internet or to consider whether the same result can be achieved by less intrusive means. The law also does not require them to confirm that the blocking measure is strictly directed against illegal content and does not have arbitrary or excessive consequences, for example, restricting access to the entire website where the disputed content was posted. The Court concluded that blocking the applicants' websites was an excessive and arbitrary measure that violated the applicants' right to freedom of expression.

Article 15.3 of the Law on Information was also previously considered in the case «Kablis v. Russia», and already in 2019 the European Court considered this provision insufficiently predictable, and its application arbitrary, which does not comply with Article 10 of the European Convention. The Court stressed that the breadth of the powers of the executive branch is such that it becomes at least difficult, if not impossible, to challenge the blocking measures in court. In cases concerning the blocking of publications calling for participation in a public event, it should be possible to obtain a judicial review of the blocking before the date of this public event. The blocked information after this date loses any value and interest, and therefore the cancellation of the blocking measure in court at this stage will be meaningless.

In addition, in all cases, the European Court concluded that the Russian legislation on blocking does not provide for effective remedies against abuse of power, which violates Article 13 of the European Convention.

Thus, already in 2019-2020, it was obvious that the Law on Information, which allows blocking information by a court and extrajudicially, does not meet international standards. However, the law has not been changed in order to ensure the protection of everyone's right to express an opinion.

On the contrary, the legislation continues to be amended with further restrictions of human rights. For example, according to the latest amendments to article 15.3 of the Law on Information, information containing not only «calls for mass riots and extremist activity, » but also «justification and (or) rationale of extremist activity, including terrorist activity» is now subject to extrajudicial blocking. The law does not clarify what actions can be considered «rationale» for such activities, which makes Article 15.3 even more vague than before and opens up new opportunities for abuse by the authorities.

Since the beginning of the war, Article 15.3 has become the main mechanism for the authorities to censor and combat the spread of alternative points of view about the actions of Russian troops on the territory of Ukraine. Based on this article, thousands of websites were blocked, including all major independent media and human rights defenders' pages on social networks. Practice has shown that this article makes it possible, without the intervention of the court, to immediately block the expression of any anti-war position, which provides the authorities with unlimited resources to fight the opposition, independent journalism, and other «unwanted» persons. Such arbitrary application of an unforeseeable law completely deprives citizens of their rights to freedom of expression.

This practice has been widely criticized by the international community. Thus, on May 2, 2022, observers for freedom of expression and freedom of the media from the United

Nations, the African Commission on Human Rights, the Inter-American Commission on Human Rights, and the Organization for Security and Co-operation in Europe published a joint statement on the importance of protecting freedom of expression in the context of the war in Ukraine, emphasizing in it «the unacceptability of blocking independent media in order to combat «fake information»."

And on May 19, a report was published by the OSCE Commissioner for Freedom of the Media, Teresa Ribeiro, in which she raised the issue of the situation with freedom of the media in the Russian Federation. Ribeiro stressed that during this reporting period (from November 25, 2021), the most severe suppression of freedom of speech and freedom of the media in the last 25 years took place.

In addition, the European Court of Human Rights, in accordance with rule 39, decided to apply an urgent interim measure in the case «**Novaya Gazeta and Others v. Russia**. The Court ordered the Russian authorities to refrain, until further notice, from actions and decisions aimed at completely blocking and terminating the activities of Novaya Gazeta, as well as from other actions that, under the circumstances, could deprive Novaya Gazeta of the right to freedom of expression. Nevertheless, the pressure continued and the editorial office of Novaya Gazeta suspended its activities in Russia.

Along with government blocks, self-censorship has increased since the beginning of the war. For example, many persons who publicly expressed disagreement with the «special operation» on the Internet deleted their publications themselves after learning about the prosecution under Article 20.3.3 of the Code of Administrative Offenses of the Russian Federation «for discrediting the use of the armed forces of the Russian Federation.» At least 191 cases are known (in about 26 of them, the authors themselves deleted the information) initiated by Russian law enforcement agencies for anti-war publications, reposts, comments, photos, and videos containing, for example:

- a photo with the inscription «NO TO WAR»;
- comments on the killing of civilians in Ukraine;
- pictures with the inscription «I AM AGAINST THE ATTACK ON UKRAINE»;
- a comment that the Russian military is waging a war in Ukraine, not a special military operation;
- a comment on possible default and use of nuclear weapons;
- a post about the Russian army dropping bombs and missiles on the territory of Ukraine.

In some cases, the materials were deleted by the administration of social networks, but soon the authorities may have the power to block such content.

The draft laws submitted to the State Duma in April 2022 provide for new grounds for extrajudicial blocks. Thus, information resources of foreign agents (in case of violation of the obligations of foreign agents), as well as information containing «fakes» or discrediting the use of armed forces, or «fakes» or discrediting the exercise of the powers of state bodies abroad, as well as calls for sanctions, can be blocked by the executive body without a court decision, which continues the repressive trend.

The formulations of these new grounds for blocking do not lag behind the existing formulations in their breadth and uncertainty. These amendments, if adopted, will further restrict the already excessively limited right of citizens to freedom of expression, without providing effective means of protection from abuse by the authorities. Most of all, these amendments will affect representatives of the civilian population who oppose the war in Ukraine, and also various human rights projects and the opposition.

Human rights standards on freedom of peaceful assembly

It is important to highlight the connection between freedom of assembly and freedom of expression, as the ECHR did in the case «Ezelin v. France, » recognizing that freedom of peaceful assembly and freedom of expression are often closely linked in practice. Restrictions on assemblies may automatically affect the right of individuals or groups to express their opinions on a particular issue. This connection is especially close on the Internet. Access to the Internet and social networks has become an important aspect for organizers of peaceful assemblies, their participants, as well as observers and human rights defenders. Blocking resources or otherwise complicating access to them restrict the right to freedom of expression of organizers and participants of public protests.

The right to freedom of peaceful assembly is enshrined in Article 21 of the International Covenant on Civil and Political Rights, as well as in Article 11 of the European Convention on Human Rights. Peaceful assemblies play a crucial role in providing an opportunity to spread ideas in society and get a reaction to them. Non-observance and failure to ensure the right to peaceful assembly, as a rule, is a sign of repression.

The obligations of states to protect the right to peaceful assembly include a **presumption in favor of the peaceful nature of assemblies**. In the case «The Christian Democratic People's Party v. Moldova, » the ECHR concluded that all assemblies should be considered peaceful in the absence of convincing evidence that the organizers and/or a significant number of participants intend to use violence or incite it. In this regard, states have an **obligation**

to distinguish between peaceful and non-peaceful participants in assemblies. **The requirements for the state in this area also include** a positive obligation to promote and protect the exercise of the right to freedom of peaceful assembly. This was also emphasized by the European Court in the case «Gun and Others v. Turkey.» Accordingly, blocking or prohibiting the dissemination of information about an assembly can be recognized as legitimate only when such information contains open calls for violence at assemblies.

Also, one of the requirements relevant for anti-war protests is the protection of the right to spontaneous assemblies. The advent of new technologies has greatly expanded the possibilities of spontaneous assemblies, and states should consider them as an expected (and not exceptional) feature of a healthy democracy. The ECHR in the case «Bukta and Others v. Hungary» noted that the state should take all reasonable measures to protect spontaneous assemblies, same as for assemblies planned in advance.

The OSCE Guidelines on Freedom of Assembly note what features legislation on assemblies, rallies and demonstrations must necessarily have**:**

- Precision. Legislatures should ensure that statutory provisions covering freedom of peaceful assembly — often contained in a range of different laws — are clear, accessible to the public and consistent with one another. This requirement was also noted by the ECHR in the case «Vyerentsov v. Ukraine»;

- Clarity regarding the mandate and procedures of decision-makers;

- Foreseeability. The ECHR noted that the requirement that any restrictions on assemblies are «provided for by law» not only implies that the restriction must have a clear basis in domestic legislation, but also applies to the quality of the law under consideration;

- A consultative approach to drafting — based on the opinion and experience of civil society;

- Periodic review.

In turn, the practice of liability for publications about assemblies, as well as blocking Internet resources that disseminate information about unauthorized public events, is separately noted in international law as illegal. The Internet and technology are playing an increasingly important role in the exercise of the right to freedom of peaceful assembly, and it is difficult to imagine an assembly in which some form of the Internet would not be used. The General Comment notes that Article 21 and related rights protect participants not only during the assembly and at the venue. Related activities are also covered, such as resource mobilization by participants or organizers, planning, dissemination of information about the upcoming event, preparation for the event and a trip to it, communication between participants before and during the assembly, broadcasting of the assembly, and leaving the assembly after it ends.

The close connection between freedom of assembly and freedom of the Internet is also noted in the OSCE Guidelines, which highlight several important points related to this topic.

Particularly important in the context of the protection of freedom of assembly is the freedom to plan, prepare and publish information about assemblies. The organizers have the right to publish and disseminate information about the assembly both online and offline in advance. As the UN Human Rights Committee noted in the Tulzhenkova v. Belarus case, websites and other electronic means used to advertise and inform about the assembly should not be restricted or blocked. Any attempt to do so usually constitutes a violation of the right to freedom of assembly.

States are required to exercise particular caution in any restriction of access to the Internet. It cannot be excluded that any interference with freedom of expression and freedom of assembly on the Internet, for example, by blocking, filtering, slowing down or closing Internet services, may constitute disproportionate interference with the exercise of these rights.

The Guidelines also remind that all international conventions apply to events taking place online, especially given the increasing importance of the Internet and social networks for the mobilization of assemblies.

The responsibility for providing barrier-free Internet access is also emphasized. Increasing access to the Internet is one of the ways in which states can partially fulfill their obligation to facilitate assemblies, and such access is increasingly becoming a right. The documents of the Council of Europe and the United Nations call for «a human rights-based approach to the provision and expansion of Internet access» and emphasize the fundamental nature of Internet access as a channel for the exercise of human rights and freedoms. Some UN advisory documents also mention (but do not define) the idea and nature of this new «human rights space» in the context of assemblies.

The General comment confirms this view by noting that States should not, for example, block Internet connections or interfere with the quality of connection because of peaceful assemblies.

Unfortunately, Russian legislation on freedom of assembly does not meet these international standards. In particular, one can note its complexity, multilevelness and inconsistency, the presence of a large number of gaps. All this creates additional obstacles for the organizers of assemblies, who cannot always quickly and accurately verify the legality of even the announcement of a peaceful assembly.

In particular, Russian legislation does not provide for the legal possibility of holding a spontaneous assembly. Any public event must be coordinated with the authorities in advance. At the same time, the terms of approval established by the law on rallies are limited to several days: depending on the format of the event, you can submit a notification no earlier than 15 or 10 days before an event. In practice, the approval procedure is often delayed or the authorities respond with a refusal (see see report of OVD-info «The art of banning»); the situation has only worsened due to the introduction of regional restrictions on holding protests against the background of the COVID-19 pandemic. The «unauthorized» status of an event leads to a number of negative consequences — from the suppression of the event and the prosecution of its participants and alleged organizers to a ban on the dissemination of information about such protests, including via the Internet.

Largely due to this state of legislation, since 2018, there has been a practice of holding authors of publications on social networks accountable for «organizing unauthorized assemblies.» The risk of blocking also makes it difficult to inform potential participants and, in general, attract public attention to the topic of the event, and also contributes to the spread of self-censorship in the media: it becomes dangerous to write about the protests. Even a repost of a video or publication calling for a rally even before the war could become a reason to hold the author of such a repost liable. Article 20.2 of Code of Administrative Offenses, to which both Roskomnadzor and the Prosecutor General's Office refer, says nothing about «calls» and punishments for them — bans on the dissemination of information on the Internet are contained mainly in the law «On Information». However, in judicial practice, the publication of information about unauthorized assemblies is often equated with their organization. The announcements about the protests have become a reason for arrests on the eve of their holding, as well as for the initiation of criminal cases. For a number of people who have become defendants in cases of repeated violations of the procedure for holding public events (Article 212.1 of the Criminal Code), statements in social networks found their way into the case materials.

The legislative basis for blocking Internet resources that disseminate information about unauthorized public events appeared back in 2014, when the Lugovoi Law came into force. Article 15.3 of the law «On Information» included a list of banned information, where peaceful actions not coordinated in advance with the authorities were put on a par with «mass riots» and «extremist activity». In the strategy of countering extremism in the Russian Federation until 2025, " unauthorized public events» occupy a prominent place and are mentioned many times. For example, in the paragraph on «the most dangerous manifestations of extremism, » along with the preparation and commission of terrorist acts, «the *organization and conduct of unauthorized public events (including protest assemblies), mass riots*» is also indicated. Since it is not explained what exactly should be considered such «calls, » in practice, information subject to immediate extrajudicial blocking may be any information about collective assemblies that are not coordinated with the authorities.

The law began to be used a few months after its entry into force. Before the verdict in the notorious Bolotnaya Square case in March 2014, the websites of three independent media were completely blocked: Grani.ru, Yezhednevnyy Zhurnal, and Kasparov.ru, as well as Alexey Navalny's blog on the LiveJournal platform. When appealing the blocks in court, it turned out that they were related to publications about unauthorized rallies. It was not possible to achieve the cancellation of the blocks through the Russian courts; the outlets appealed to the ECHR. In the summer of 2014, Roskomnadzor, under threat of blocking, achieved the removal of material about the upcoming «March for the Federalization of Siberia» (published before the possible start date of approval). The march group in VKontakte was blocked, and the media outlets that wrote about the block recieved warnings. In December of the same year, groups in social networks dedicated to the assembly in support of Alexei and Oleg Navalny were blocked (the organizers also had not yet had a legal opportunity to file a notification).

Over the following years, the number of blocks for «calls to participate in mass events» grew rapidly.

In December 2020, amendments to the law «On Information» were adopted in high-speed mode: owners of social networks were obliged to monitor and restrict access to banned information, including «containing calls for... participation in public events held in violation of the established procedure, » and «information aimed at inducing or otherwise involving minors in committing illegal actions that pose a threat to their life and (or) health or to the life and (or) health of other persons.» Administrative liability was introduced for non-compliance with this requirement — the amendments came into force on January 10 and two weeks later they began to be applied.

The fight against the dissemination of information about the rallies in social networks and the media intensified against the background of mass protests in January 2021. Then all the laws and prohibitions on the dissemination of information adopted by that time, threats of blocking and administrative fines, as well as simultaneous pressure on the media, social networks and users, were used.

Before the first large-scale rally in support of Alexei Navalny in January 2021, the Prosecutor General's Office announced *measures of prosecutorial response after «identifying calls to participate in illegal mass events on January 23*, 2021.»

Roskomnadzor sent a warning to the owners of social networks that they would be fined under Article 13.41 of the Code of Administrative Offenses and mentioned several provisions of the legislation at once, which, according to the agency, would be violated if information about the protests was disseminated: «*the involvement of minors to participate in unauthorized mass (public) events* ... *including in the context of a pandemic, carries risks of harm to life and health.*» Also on the day of the protest rally on January 31, the agency stated: «*Based on the requests of the Prosecutor General's Office and Roskomnadzor, the administrations of social networks block access to false information, with inflated indicators about the number of participants in illegal rallies, about the alleged facts of violence and clashes, the deaths of participants in the rallies.*»

Many social networks have blocked pages and accounts with banned information about the protests — VKontakte blocked dozens of pages dedicated to the event in different regions; Roskomnadzor reported on blocks of TikTok and Instagram on January 22. A few days after the protests, RKN issued a new warning*: «Social networks Facebook, Instagram, Twitter, TikTok, VKontakte, Odnoklassniki, and YouTube video hosting will be fined for failure to comply with the requirements to stop the dissemination of calls for minors* *to participate in unauthorized rallies on January 23. Despite the request of the Prosecutor General's Office and the notification of Roskomnadzor, these Internet platforms did not remove a total of 170 illegal calls in a timely manner.»*

Before the protest with flashlights on February 14, Roskomnadzor put pressure on the media, seeking to remove news about upcoming events, which were equated to calls for «participation in events that take place in violation of the established procedure.» One of the websites, the Spectr outlet, was blocked after all because it allegedly contained illegal calls.

The next wave of protests — and with it a wave of blocks for political reasons — came in April 2021:

- **On March 31,** Alexei Navalny declared a hunger strike in the penal colony, demanding medical assistance;
- On **April 16**, the Moscow Prosecutor's office filed a lawsuit to the court demanding that the Anti-Corruption Foundation and the regional offices of Alexei Navalny be recognized as extremist organizations;
- On **April 18**, Navalny's team announced rallies demanding that doctors be admitted to the opposition figure, whose health situation, according to doctors, was becoming critical;
- On **April 19**, the Prosecutor General's Office issued a warning about the impermissibility of calls to participate in unauthorized assemblies with reference to Article 20.2 of the Code of Administrative Offenses on violation of the procedure for holding public events;
- **On April 19**, Roskomnadzor demanded from the YouTube video hosting to block the video of Navalny's team «The final battle between good and neutrality, » in which the rallies were announced. After that, Navalny's press secretary, Kira Yarmysh, was arrested for 10 days for «organizing» an unauthorized rally through calls on the Internet. By that time, Yarmysh had already been under house arrest for two and a half months due to the «sanitary case» and could not use the Internet;
- Protests were **held** on April 21.

Roskomnadzor's struggle with YouTube video hosting — the main media platform of Navalny's team — continued throughout 2021. In fact, in July, RKN demanded to remove the channels of the associates of the opposition politician Leonid Volkov, Vladimir Milov, Georgy Alburov, and Vyacheslav Gimadi. The request contained a threat: according to the RKN, if they do not delete the content of the channels, «Google may be forced to block the content.» The demand came from the Prosecutor General's Office, which found at once several types of «banned information» described in Article 15.3 of the law «On Information» in the video materials.

VKontakte was fined twice, for a total of 3 million rubles, including for links to Youtube. Google, Facebook and Twitter have received a total of 16 protocols from Roskomnadzor related to the refusal to remove content banned in Russia and fines of tens of millions of rubles — including for calls to go to «unauthorized rallies.»

In addition to social networks, individual sites and projects have also suffered due to blocks related to the «calls»:

- The student magazine DOXA, under threat of blocking, deleted its video message with a call not to be afraid of expulsion from the university for participating in a rally: Roskomnadzor decided that the video contained «incitement or other involvement of minors in committing illegal actions that pose a threat to their life and health, » and entered it into the register of banned information. Despite the fact that the editorial board deleted the video, a criminal case was later opened.

- After the elections in September, the Communist Party, under threat of blocking, removed from the website the announcement of a meeting with MPs on Pushkin Square.

- Among the grounds for blocking the OVD-Info website there also was an article about protests in support of Navalny.

Thus, it can be concluded that even before the war in Ukraine, Russian legislation did not meet the criterion of «quality of law», and law enforcement was often arbitrary and disproportionate, which, of course, did not meet international standards in the field of freedom of assembly.

The UN Special Rapporteurs on Freedom of Assembly and Freedom of Expression also asked in their communication to the Russian authorities after the winter protests of 2021 to explain how Internet restrictions and blocking were necessary, proportionate and consistent with Russia's international legal obligations. However, the situation with blocks of content related to peaceful assemblies has not improved — even the other way around.

After the outbreak of the war, with the introduction of Article 20.3.3 in the Code of Administrative Offenses, and Article 207.3 in the Criminal Code of the Russian Federation, the practice of liability for publications about assemblies only worsened. Now the authors are being held liable not only for «organizing» rallies, but also for «discrediting the Armed Forces of the Russian Federation.» We are aware of at least 22 indictments for such publications.

The rulings were made because people posted videos, posts and reposts on their social media pages with calls to participate in anti-war assemblies. In fact, the Soviet District Court of Voronezh considered that as a result of such publications, «the credibility of the special military operation could be undermined.» Roskomnadzor also announced the blocking of over 38 thousand messages calling for protests against the war in Ukraine. It is important to emphasize that people often delete such posts on their own, as part of self-censorship — without waiting for the reaction of Roskomnadzor.

We would like to emphasize once again that in accordance with international standards in the field of freedom of assembly, the legislation and policy of the state should ensure the possibility of barrier-free use of the Internet — especially social networks — for the preparation and organization of peaceful assemblies. However, the legislation and practice of the Russian Federation are infinitely far from meeting these standards.

BLOCKING IN VIOLATION OF RUSSIAN LAWS

Existing Russian laws, even those that, according to the decisions of the ECHR, do not comply with international standards and violate the right to freedom of expression, the right to freedom of assembly and legal protection, are often violated during the blocking of Internet resources in Russia. «*Our law enforcement is very different from what can be indicated in the law*, » says Artem Kozlyuk. «And *various supervisory agencies interpret the norms in their own way, which in themselves raise many questions. The absurd is followed by more absurd.»* In extrajudicial («prosecutor general») blocks, according to his observations, the provisions of the law are violated more often. Roskomnadzor can add the resource to the Unified Register at the request of the Prosecutor General's Office, which was sent a year ago — which does not comply with the law «On Information». In the first days of the war, according to a study by Roskomsvoboda, many media were included in the Register twice — based on different decisions of the Prosecutor General's Office.

In addition, blocking decisions are most often made without an invitation of the site owners or administrators, usually with a comment that the blocking «does not affect their rights.» The lawyers of Roskomsvoboda received an explanation from the Supreme Court that when making a decision to block the site, the court should invite the owners of the site to the hearing, that is, to ensure equality of the parties. Before the start of the war, according to Artem Kozlyuk, lawyers who knew about this explanation had every chance to return the case for a review of the decision of the lower courts. After February 24, cases of blocks became widespread and at the time of writing the report, the new practice has not yet developed.

OVD-INFO

One of the striking examples of the situation described in the previous paragraph was the blocking of the OVD-Info website on December 25, 2021 based on the decision of the Lukhovitsky District Court of the Moscow Region under Article 15.1 of the Law «On Information» (149-FZ).

On December 13, 2021, a notification from the Lukhovitsy town prosecutor's office came to the project's email address with a request to appear the next day, December 14. The lawyer of OVD-Info Anastasia Samorukova managed to get to the Lukhovitsy prosecutor's office within the specified period, but she was not allowed to familiarize herself with the case materials. The next day, the prosecutor's office appealed to the court.

In the verdict published on the court's website on December 31, it is said that «*the representative of the interested person, duly notified of the time and place of the hearing, did not appear in court,*» and also that «*the persons to be involved in the case as defendants have not been identified, information about their name and location has not been submitted to the court; however, it is known that there is an IP address.*» It is separately mentioned that the IP address «is located in San Francisco USA». At the same time, there is a mention in the court verdict that OVD-Info is included in the register of foreign agents (in which the names of the co-founders of the project are indicated).

The published court decision does not give a clear understanding of the reasons for blocking the site. It lists five materials, including those from 2018, but it is not individual pages that are subject to blocking, but the entire site, which does not comply with the norms of the law «On Information.» The Roskomsvoboda project, after analyzing the blocking technology, comes to the conclusion that «*since no stub page appears when entering the site, the blocking may concern* *some specific or several links, and not the site itself, and access is restricted via HTTPS*.»

The decision mentions the ANO Center for the Promotion of Humanitarian Expertise «Independent Expert.» According to the «comprehensive psychological and linguistic research» conducted by the Center, the materials of the OVD-Info website contain justification of terrorism and extremism, as well as «*convincing potential recipients of the need to participate in unauthorized protests, as well as violate current legislation and ignore the legitimate demands of law enforcement officers and other authorities*.»

The prosecutor present at the court session supplemented the written requirements of the prosecutor's office with the conclusions «*on the systematic posting on the website of the OVD-Info media project on social networks of information aimed at justifying the activities of extremist and terrorist associations, materials justifying the actions of participants in such organizations, as well as information forming for an indefinite circle of Internet users motivation and readiness to participate in public events held in violation of the established procedure*.» And in general, he came to the conclusion that the activities of OVD-Info are aimed at «propaganda of terrorism and extremism on the territory of the Russian Federation.»

In accordance with the requests of the prosecutor's office, the Lukhovitsky court concludes that «*the content [of the site materials] is capable of forming an idea in a significant part of the audience about the permissibility of committing crimes, including of terrorist orientation, an idea about the possibility of obtaining public support and approval, as well as the status of a „political prisoner“.*» At the end of this document, before the formula of the court decision («to recognize the information… as prohibited for distribution on the territory of the Russian Federation»), its general motivation is given, worthy of special mention: «*Ensuring free* *access to information contributes to the formation of public opinion about the possibility of unpunished commission of crimes and administrative offenses, undermines the authority of the state authorities of the Russian Federation and the current legislation.*»

Looking at the published court decision, it is obvious that it is not based on the recognition of any specific materials as prohibited, but on the assumption that the materials of the OVD-Info website can form an idea of the permissibility of crimes. Based on this conclusion, it was decided to block not individual pages, but all the Internet resources of OVD-Info. Yandex removed the link to the OVD-Info website from the search results, and soon the project's social media accounts were requested to be blocked.

International NGOs, including Human Rights Watch, Amnesty International, Civil Rights Defenders, Reporters Without Borders,Accessnow, CIVICUS, Article 19, condemned the blocking of the project's website. The European Union also criticized this decision. A request was sent by the Human Rights Council, in response to which the Russian Federation simply retold the history of the blocking of the site and indicated that access was restricted on the basis of Article 15.1 of Federal Law No. 149-FZ of July 27, 2006 «On Information, Information Technology, and Information Protection», noting that notifications of blocking and the court hearing were compliant with the law.

International organizations also spoke about the pressure on non-state media covering the war in Ukraine. Amnesty International's Director for Eastern Europe and Central Asia, Marie Struthers, said that «*after Russian tanks entered Ukraine, the authorities switched to a scorched earth strategy that turned the Russian media landscape into a wasteland*.» It is worth mentioning that on May 11, the Russian-language website of Amnesty International (eurasia.amnesty.org) was blocked by Roskomnadzor. Similar statements were also made by CIVICUS, HRW, Article 19, Human Rights Defenders, Access Now, The National Endowment for Democracy, and other non-profit organizations.

Reporters Without Borders have called on Meta (Facebook and Instagram), Google (YouTube), Twitter, and Telegram not to comply with the draconian requirement of Roskomnadzor to delete accounts of the OVD-Info website. In addition, Reporters Without Borders, using the technology of the Collateral Freedom mirror site, created an exact copy of the Meduza site and invited all independent media blocked by Russian censorship to contact them in order to open «mirrors» on reliable content delivery networks (CDN or Content Delivery Network — geographically distributed network infrastructure which is difficult to block).

Many international associations of journalists have also expressed their dissatisfaction with the pressure on independent media: global network of the International Press Institute, Secretary General Anthony Bellanger of the International Federation of Journalists, and the Committee to Protect Journalists have published statements against the attempt of the Russian authorities to censor independent media covering the invasion of Ukraine.

Despite numerous calls from the international community to respect and protect the right of people in Russia to freely receive and disseminate information and express various or critical views, control over independent journalists and freedom of speech (including by blocking) in Russia is only getting tougher. In general, it was not possible to get any reaction from the Russian authorities.

FINANCIAL CONSEQUENCES OF BLOCKING FOR INDEPENDENT PROJECTS

Blocking scares donors

Regardless of the formal reason for blocking, private donors see risks for themselves and stop supporting independent projects. Sometimes, seeing that the site does not open, just decide that the project has closed. The outflow of donations was primarily influenced by news about the persecution of FBK (Anti-Corruption Foundation) donors, as well as the leaks of databases of their supporters, and the threat of persecution of donors of projects and organizations whose activities were deemed undesirable on the territory of the Russian Federation — the sites of projects and organizations deemed undesirable are blocked by Roskomnadzor at the request of the prosecutor's office, and the projects themselves suspend the acceptance of donations, to protect the donors. Confusion due to the abundance of statuses given to undesirable projects, formal reasons for blocking, as well as constant changes and tightening of legislative acts leads to the fact that the very fact of blocking of a site hits the project donors hard.

Blocking also affects the cooperation of NGOs with business partners: joint projects or support from companies are either impossible under blocking conditions (subdomains of special projects are blocked together with the main site), or they lose greatly in efficiency and audience. And the companies themselves try to avoid unnecessary risks from cooperation with such projects and media.

Software for accepting donations is disabled

Blocking sites leads to the shutdown of payment services, thanks to which projects accept donations from bank cards. For online projects, this is the main way to receive donations. In most cases, this is a technical limitation — the rules of the services prescribe the requirements for the site and if the site does not work, the service has the right to terminate the service. Here’s what these rules look like, for example, on the YooMoney website:

11.8. The Counterparty’s website must comply with the following requirements:

11.8.1. The website should contain the following current information: a description of Counterparty services/catalogue of Products and their price, conditions, procedure, terms, delivery regions for Products (services, works), terms and procedure for the return of Products, refuse Products and Payment Refund, full company name, TIN, legal and actual addresses, telephone number and e-mail of the Counterparty, user agreement that take into consideration requirements of the clause 2.15 of the General Terms and Conditions (if applicable), client data confidentiality regulations, appeal to the clients on saving copies of the documents that confirm Products payment, appeal to the clients on methods and means of their data protection, links to Products producers websites, terms of warranty provided by the Counterparty;

11.8.2. All pages that are related to the implementation of the Products must be under a single domain name. At the same time, if the Counterparty is not an owner of the domain name, it must provide documents confirming the legal grounds for using the website;

11.8.3. The website must be maintained in working state. All internal links of the website must work and be adequately processed;

11.8.4. The website should not contain information (textual, graphic or any other kind), the dissemination of which is contrary to the current legislation or morality standards, as well as links to websites containing such information.

Such information includes, for example: propaganda in any form of violence, drugs, terrorism, ethnic hatred, prostitution, etc.

Accordingly, when the services are disabled, payment forms stop working and regular subscriptions to donations are disabled.

Block bypass services also affect the acceptance and processing of donations — in many cases, a donor who has a VPN enabled (and this is often the only way to access the website of a blocked publication) will not be able to complete the donation process. This is how the Mediazona project, which lost many donors due to blocks, described the situation on March 16, 2022:

In the situation in which we all found ourselves today, when making a donation, we have to take into account a whole host of factors: in which country you are located, whether you use a VPN or not, which bank issued your card, whether it fell under sanctions, whether you have a MasterCard, Visa or something else — all this can interfere with a transaction and for each case now we are trying to find a solution.

Over the past few days, we have lost a huge number of subscriptions. Due to sanctions and the withdrawal of the largest payment systems from Russia, more than half of regular payments have been canceled, they will never work again.

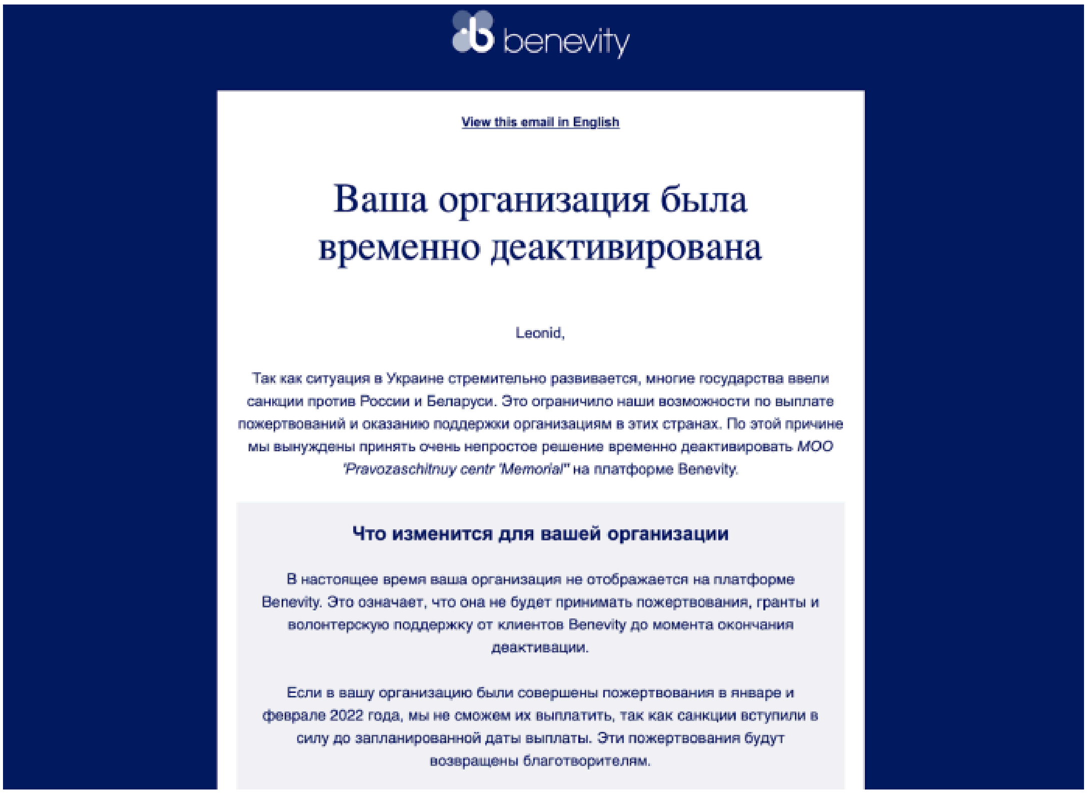
Sanctions against the financial and banking system in Russia

During the war, most independent and human rights projects in Russia found themselves between two fires: on the one hand, they are under pressure from the Russian state and face restrictions within the Russian Federation, on the other, they are affected by the sanctions against Russia. The latter led, first of all, to technical problems with accepting payments (for example, as a result of disabling Apple Pay and Google Pay), as well as to disabling services that were used to communicate with donors (for example, Mailchimp). Due to these restrictions, some services were forced to greatly reduce their funding and restructure their work by accepting donations in war conditions.

- Apple and Google Pay: along with disabling them for Russian bank cards, all regular subscriptions previously issued using these services are also disabled;
- Foreign services (for example, Stripe) stopped serving Russian cards, and those projects that used these services had to refuse donations from Russian cards. In particular, Meduza did it:

> ☒☒**Dear readers! We were forced to turn off accepting payments from Russia. We hope that this is a temporary measure. But you can still transfer money to us from anywhere else on the planet. Please tell your friends and acquaintances living abroad about this. Meduza needs support. More than ever.**

- Russian services stopped working with cards of foreign banks — all subscriptions issued from cards of foreign banks were canceled; this affected not only online projects, but also the whole sphere of charity, which lost about half of donations.
- International crowdfunding platforms (GlobalGiving and Benevity) have suspended payments to projects from Russia and Belarus, primarily due to the inability to transfer money from a foreign bank to Russian accounts of organizations.



View this email in English

Ваша организация была временно деактивирована

Leonid,

Так как ситуация в Украине стремительно развивается, многие государства ввели санкции против России и Беларуси. Это ограничило наши возможности по выплате пожертвований и оказанию поддержки организациям в этих странах. По этой причине мы вынуждены принять очень непростое решение временно деактивировать *МОО 'Pravozaschitnuy centr 'Memorial'"* на платформе Benevity.

Что изменится для вашей организации

В настоящее время ваша организация не отображается на платформе Benevity. Это означает, что она не будет принимать пожертвования, гранты и волонтерскую поддержку от клиентов Benevity до момента окончания деактивации.

Если в вашу организацию были совершены пожертвования в январе и феврале 2022 года, мы не сможем их выплатить, так как санкции вступили в силу до запланированной даты выплаты. Эти пожертвования будут возвращены благотворителям.

PERSPECTIVES FOR THE «SOVEREIGN RUNET»

By the end of February 2022, the trajectory of further restrictions on freedoms in the Russian segment of the Internet was more or less clear and most experts agreed in their forecasts.

Among the figures of pro-government structures, the discussion of new forms of censorship continued, which were often presented as the result of public consensus. For example, entrepreneur Igor Ashmanov proposed creating another registry of «toxic content», which includes, in particular, «information about violence, the danger of vaccinations, radical feminism, refusal to have children, encouragement of LGBT, and bestiality.» He was supported first by the chairman of the Human Rights Council, Valery Fadeev, and then by Vladimir Putin, who instructed his administration to study Ashmanov's idea and «take appropriate support measures if necessary.» The «Safe

Internet League» was also active, which allegedly recorded «preparations for interference in elections» through the purchase of accounts in social networks.

The main tools and technologies of the «sovereign Runet» as a whole have already developed. And although not all of them have been used at full capacity yet, experts have a feeling that it is now possible to block almost any information. Experts interviewed by the Mediazona project in September 2021 were surprised to note the approaching isolation. Here is how Mikhail Klimarev, director of the Internet Protection Society, commented on the situation:

«It turned out that they can. Well, that is, we thought not, but it turned out that they can. In theory, by definition, nothing can be blocked on the Internet, because it is a fully connected graph, and if there are any obstacles in the way of this graph, you can always find workarounds. Especially with the modern development of cryptography. Of course, we will come up with something that will then be widely used. But at the moment it turns out that Roskomnadzor can block, including protocols.»

Technical ways to bypass the blocks exist, but they are all too complex to be widely available. «I don't think anyone will run [after ordinary users] for such things, » Klimarev says.

The experts of the OVD-Info round table expressed slightly more optimistic views. So, for example, Artem Kozlyuk (Roskomsvoboda), noting that the blocks have become technically more effective, thoughtful and «literate, » nevertheless came to the conclusion that the fight is not over yet: «*All this can be done for a short period of time. It is quite difficult to block a resource for a long time if it resists. It's always a technology fight. And you can disguise your traffic in order to bypass DPI tools, and come up with new ways of circumventing, as TOR does, which began distributing information about active nodes to its users*.» However, according to Kozlyuk, such a struggle leads to the degradation of the Internet in Russia — to the decline of related businesses, slowing down of communication channels, and monopolization of the market.

After February 24, the blocks became total. No new tools and concepts were created, but the existing ones began to be used with renewed vigor. This is especially true in the context of «fakes» as a justification for blocking, which used to be applied mainly to information about the coronavirus. Moreover, in relation to «false information» a stable definition appeared, first given in the press release of Roskomnadzor directly on February 24: this is any information that is not confirmed by official sources (authorities and state media).

Among all the blocks, «prosecutorial» ones — that is, those that do not require prior notification of the site owner and, as a rule, are politically motivated — have almost doubled compared to the same period in 2021. Despite Roskomnadzor's willingness to cut off the Russian segment from the global network, there were sources of information in the pre-war situation that were not fully controlled by the Russian authorities — in particular, this applies to such IT giants as Google (and Youtube), Meta (Facebook, Instagram), Telegram, and some others. However, after the outbreak of the war, Meta was recognized as an extremist organization, and Google is closing its office in Russia. According to the law «on landing, » this means that Roskomnadzor can block it. So far this has not happened, but Damir Gainutdinov believes that this lull is temporary: «*It is difficult to make forecasts, but it seems to me that further measures will be taken now with regard to global platforms that have not yet been completely blocked. The big question is with Telegram, which is now the main media platform, as well as with Youtube*.» In his opinion, the lull may be due to the fact that the state itself uses these platforms for propaganda, but sooner or later the aggressive threats of Member of Parliament against them will be put into effect. Artem Kozlyuk also talks about the imminent closure of Youtube in an interview with the Yekaterinburg Online newspaper: «*Not only us, many predicted that YouTube would be blocked — and that it would be the last to whom they would come. Because it is a video hosting, it is a social service, the most important for Russians. It has bloggers with millions of subscribers who specialize in a variety of issues. Travel bloggers, beauty bloggers, children's content, entertainment, educational — any*.»

DPI technologies tested on Twitter can slow down video hosting in such a way that it will be almost impossible to use it. At the same time, Google and Youtube have already disconnected Russia from their payment systems, so bloggers with more than a million of subscribers can no longer use the service to earn money. Thus, technical means of isolation of the Runet are not as important as financial instruments, the absence of which prevents the development of the Russian segment of the network.

At the same time, the pressure on users from the state is growing. «*It seems to me that the authorities will return to the mechanism of intimidation of users*, » says Damir Gainutdinov.«*They will try to prevent the dissemination of information, work with propaganda, and not technically block access*.» Intimidation — such as punishment for «public dissemination of deliberately false information» about the use of the Russian army with up to 15 years in prison, as well as sharply increased size and number of fines — leads to the fact that many media outlets suspend their activities or dissolve editorial offices, while others engage in self-censorship. By and large, the sanctions, which deprive Russian users of software and equipment, and many projects of donor money, do not weaken, but on the contrary, strengthen the position of the Russian authorities and, in particular, Roskomnadzor as the main body of online censorship.

«*Blocking depends not only on Roskomnadzor and legislators*, » says Artem Kozlyuk, «*But also on technological progress and on the reaction of the resource itself, as well as on the public reaction. Consolidation of opinion, an open position, and a public campaign can also affect the situation with blocks in Russia.»* Even before the war, the activities of the Prosecutor General's Office and Roskomnadzor did not cause a mass reaction in society — which in many ways helped censorship grow to its current scale. After the outbreak of the war, many media outlets, as well as individual activists and human rights defenders, were forced to suspend their activities or move outside the Russian Federation.

At the same time, the statistics of VPN downloads has grown significantly, which means that a large part of users still seek to receive independent information. However, the difficulty of access certainly affects the dissemination of an alternative news picture. After the outbreak of the war, blocking became one of the main tools of censorship, as they are aimed primarily at those who disagree with the official position of the state about the war in Ukraine. Along with administrative and criminal prosecution, laws on «foreign agents» and «undesirable organizations, » blocks work to suppress dissent. In these conditions, the support of the international community and large companies, especially in the IT field, is more important than ever for those who are ready to engage in information resistance: access to information is directly related to access to technologies and software, including payment systems.

SUMMARY

Blocks of Internet resources as a tool of political censorship appeared back in 2012. If at first, the blocks were possible only after a court decision and were applied mainly to those websites that contained information dangerous for children (pornography involving minors, selling of drugs, ways to commit a suicide, etc.), then in the following ten years, they have acquired a clearly political character and have become directed at the restriction of civil rights and freedoms — freedom of expression, freedom of assembly. The first large bursts of political censorship appeared in 2014, and since then the tools and scale have only expanded. At the same time, blocks have serious consequences for organizations: financial, organizational, reputational.

Largely due to the blocks, there is systematic censorship in Russia, the existence of which state bodies deny, accusing of censorship, on the contrary, foreign Internet platforms when they restrict access to the accounts of official Russian media. The infrastructure of large-scale censorship on the Internet has appeared thanks to new technologies and legislation, as well as the long-existing rhetoric about the sovereign Runet, which allows all new initiatives to be pushed through.

The gradual evolution of the legislation on blocking, from «the law on protecting children from information», to the Lugovoi Law and laws on «foreign agents/undesirable organizations, ” makes clearly visible the connection of blocks with other types of freedom restrictions, and the desire of the authorities to control the flow of information. In fact, blocks and requests to delete information related to large opposition organizations are especially frequent. By 2020, the regulatory and technological support for the isolation of the Runet had been generally completed.

In spite of international standards in this area, in Russia, the blocks often occur with significant violations of both international and domestic norms — some media get into the registry twice, site owners are often not notified about blocking, the whole sites or even domains are blocked instead of individual pages that contain banned information.

In recent years, thanks to state commissions, a large number of special programs and systems has been developed that give to the authorities an easier way to search and limit the access to Internet resources. For example, the «Revisor» system; and also the «technical means to counter threats» (TMCT), through which most traffic passes and which allows to slow down and block various sites; and also, artificial intelligence systems and neural networks to automate content search. In addition, the technical possibility of blocking VPN services has recently appeared.

Blocks also occur manually, with the help of various pseudo-public organizations, on the initiative of various departments. Mass blocks have already become routine work for the state, whereas aimed ones depend on the decisions and opinions of specific actors. Examples of blocking by «order from above» are Alexey Navalny's projects and Open Russia projects, sites and accounts of which were persecuted in various ways and for various reasons.

By the time of Russia's invasion of Ukraine, all legislative instruments had already been developed and widely used, which made it possible to clean up the information field in a few weeks, when all non-state socio-political resources were blocked. Already on February 24, a new wording appeared that allows to use the legislation on blocking literally for any resource: from this day, all information is considered «false» if it is not supported by «oficial, " state sources. Moreover, not only Russian-language media are blocked, but also foreign ones, and major media platforms, primarily the social networks. Since the beginning of the war, self-censorship has also increased in such a situation — people do not post or delete anti-war publications, fearing administrative and criminal liability. The new legislation on extrajudicial and mirror blocking, already adopted in the first reading, will give the authorities even more tools for control and censorship. The situation is practically not covered, the data on the blocks is gathered only by few activists. Since the start of the war, it has been increasingly difficult for them to receive the help of the international community, and for the ordinary users from Russia, to access the technological resources that allow them to circumvent the restrictions.

More to read

Democratic Russia? Historian explains what led to fizzling out of Russia’s grassroots tradition

Repression in Russia in 2023. OVD-Info overview

In contrast to its forerunner, 2023 didn’t grab headlines with massive protests or numerous arrests. However, it would be a mistake to interpret this as the cessation of dissent...